(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2000 (06.07.2000)

PCT

(10) International Publication Number
WO 00/39731 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US99/30678

(22) International Filing Date:
21 December 1999 (21.12.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/113,706 24 December 1998 (24.12.1998) US
09/472,100 20 December 1999 (20.12.1999) US

(71) Applicant and
(72) Inventor: WHITFIELD, Henry [US/US]; 2490 Agnes Way, Palo Alto, CA 94303 (US).

(74) Agents: GLENN, Michael, A. et al.; Glenn Patent Group, 3475 Edison Way, Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

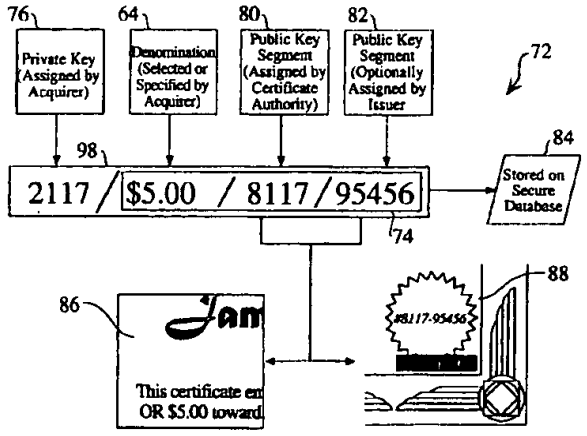
Published:
— *With international search report.*

(48) Date of publication of this corrected version:
15 February 2001

(15) Information about Correction:
see PCT Gazette No. 07/2001 of 15 February 2001, Section II

[Continued on next page]

(54) Title: SECURE SYSTEM FOR THE ISSUANCE, ACQUISITION, AND REDEMPTION OF CERTIFICATES IN A TRANSACTION NETWORK



(57) Abstract: A transaction network contains a networked certificate authority, by which one or more virtual certificates may be remotely defined and stored, such as by an issuer user through an issuer web portal interface. An acquirer user, through an acquirer web portal interface, may acquire one or more virtual certificates, which contain a public key portion, as well as a corresponding private key, which is established at the time of acquisition, and is stored at the certificate authority. At a redemption location associated with an acquired certificate, the acquirer (or an alternate recipient of an acquired certificate to whom the acquirer has communicated the established private key), submits the certificate information, along with the established private key, to redeem the certificate.

WO 00/39731 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE SYSTEM FOR THE ISSUANCE, ACQUISITION, AND REDEMPTION OF CERTIFICATES IN A TRANSACTION NETWORK

FIELD OF THE INVENTION

The invention relates to the field of certificate systems. More particularly, the invention relates to a certificate system for the controlled and secure issuance, acquisition and redemption of single-use certificates in a transaction network.

BACKGROUND OF THE INVENTION

The quickly expanding internet provides a variety of on-line commerce structures and processes, allowing online browsing and sales through a variety of dedicated retail web-sites, which typically offer one or more products. An inventory of products, which are typically stocked at one or more remote warehouse or related retail locations, are offered for sale through a web site. A purchaser, upon selecting a desired product, typically enters purchase information, such as credit card information and shipping information. Upon credit card authorization, typically when the items are shipped to the designated shipping address, the authorized card information is used to transfer monetary funds from the purchaser's credit account to the seller's bank account. While such on-line commerce systems provide adequate purchasing opportunities for buyers who have access to the Internet, typically for the purchase of smaller items which are readily sent (*e.g.* such as through postal services), such online commerce does not typically allow a buyer to conveniently pick up merchandise locally.

As well, there is an increasing development for systems which enhance the automation of on-line and off-line commerce, as evidenced by on-line payment systems, point of sale terminals, and debit cards. Related documents include *Making the World Go Round (Online Payments),* Internet Business, no. 24, p. 28-30 (Jan. 1999); *Wireless Point of Sale Terminal for Credit and Debit Payment Systems,* Conference Proceedings, IEEE Canadian Conference on Electrical and Computer Engineering, (1998); *Is Off-line Debit about to Derail?,* ABA Banking Journal, vol. 89, no. 9, p. 66,68,70 (Sept. 1997); *1998: Year of*

the Debit Card, Bank Systems & Equipment, vol. 24, no. 11, p. 16-18 (Nov. 1987).

I. Krsul, J. Mudge, and A. Demers, *Method Electronic Payments that Prevents Double-Spending,* U.S. Patent No. 5,839,119 (17 November 1998) and corresponding European Patent Application No. 0833285, *Method and Product for Generating Electronic Tokens,* (filed 25 September 1997) disclose a "method of generating electronic monetary tokens that supports off-line transactions while preventing double-spending. Generation of electronic token halves by a financial services provider begins in response to a request from a buyer to generate monetary tokens to be used with an identified seller. First, the financial services provider generates a plurality of electronic monetary tokens. Second, the provider splits each monetary token into two electronic token halves and associates with each the same serial number. These electronic token halves when combined recreate the electronic money token from which they were generated, but buy themselves neither electronic token half has any value. Nor can either electronic token half by itself be used to create the electronic monetary token without the token half's mate. After splitting all the monetary tokens, the services provider assigns a half of each electronic token to the seller and the other half of each electronic token to the buyer. The buyer and seller can now engage in multiple transactions off-line of the financial services provider". While Krsul et al disclose a method of generating electronic monetary tokens, they fail to disclose a system for issuer-defined virtual certificates which are acquired on-line during a first transaction in which an acquirer establishes a secure private key that is associated with the acquired certificate, and are then selectively redeemed off-line, using the re-submitted private key to authorize the redemption transaction with the on-line system, and to revoke further use of the acquired certificate.

K. Ginter, V. Shear, F. Spahn and D. Van Wie, *Systems and Methods for Secure Transaction Management and Electronic Rights Protection,* U.S. Patent No. 5,915,019 (22 June 1999) disclose systems and methods "for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control

and/or m t r or oth rwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway".

Gift Certificate Systems. Traditional gift certificates are typically offered by a small percentage of retail stores. There are often major costs associated in the creation and distribution of paper-based certificates, as well as in the management of in-store redemption. Consumers are thus presented with a narrow range of merchant outlets where certificates can be redeemed. The buyer often has to travel to the store to buy the certificate, and then the recipient has to wait until the buyer sends the paper-based certificate to the recipient. As well, there is often no authorization control on the redemption of the paper-based certificate. Paper-based certificates are often treated as cash, and a lost or stolen certificate usually will not be refunded to the buyer or recipient.

Some dedicated network locations, such as web sites which offer goods and services for a single entity, typically offer the purchase of pre-printed and inventoried paper-based gift certificates, which are typically purchased on-line by a buyer, and then are typically sent to a desired recipient.

As well, aggregated web sites which offer multiple goods and services from multiple sources often offer the similar online purchase of generic certificates, which may then be redeemed on-line by a recipient, such as towards the purchase of inventoried goods, which are subsequently sent to the recipient redeemer.

As well, some web-based companies, such as located at "www.giftpoint.com" and "www.giftcertificates.com", have recently been established to sell a variety of gift certificates, which inventory and offer for sale a large number of pre-printed gift certificates, typically related to nationally traded products and services (*e.g.* such as redeemable certificates from Gap Stores, Inc. or Wal Mart, Inc.). While such sites allow a buyer to purchase a certificate online, the range of merchants they

support is only a small subset of the alr ady small number of merchants who offer traditional paper-based c rtificates. Such sites inv ntory th paper-bas d gift certificates, and offer the certificates to buyers through the web site. When a paper-based certificate is purchased through the site, funds are typically transferred from the buyer at the time of the transaction, and the stocked paper-based certificate is then sent to the designated recipient. While such sites offer a variety of gift certificates for purchase, the certificates are required to initially be established (*i.e.* printed and recorded) by each of the businesses, and are then transferred to the site (such as by a purchase transaction), where they are inventoried. While large business entities may have already established paper-based certificates, small issuers (*e.g.* such as small or localized businesses) often do not have certificate systems of their own.

A similar on-line business, located at "www.gifttracker.com", provides gift certificates which may be purchased online and redeemed locally. The site provides a redemption and retail location search engine, by which an online shopper may search for certificates, based upon redemption type (*e.g.* such as by toys, books, sports equipment, or women's apparel), as well as by location (*e.g.* such as by entering by zip code). For a given product type, an online shopper typically enters a zip code (such as the zip code of the shopper, or the postal zip code of a potential recipient of a gift certificate). Based upon the entered postal code, the search engine determines gift certificates which may be redeemed locally within the submitted postal area. While the certificate system implemented by gifttracker.com provides the online purchase of certificates which may be redeemed locally, the system requires an inventory of printed certificates which are supplied by the issuers (*e.g.* such as conventional printed certificates available from large chain stores). After an on-line purchase transaction, the pre-printed certificates are then packaged and sent to a designated address (*e.g.* such as the acquirer's address, or an alternate recipient address). Once a pre-printed certificate arrives, such as by a conventional mail service, the pre-printed certificate is then taken by the recipient to a corresponding store. The site does not allow the on-line creation of a remote, electronic gift certificates, such as for issuers that do not have pre-printed certificates. As well, the system inherently requires an associated inventory and distribution system for the pre-printed gift certificates.

Another web-based company which sells certificates is located at "www.webcertificates.com", which enables recipients of a certificate to redeem the certificate from a wide variety of on-line merchants. The site creates a certificate which is similar to a virtual credit card, which is then readily accepted by a wide variety of on-line merchants who accept credit cards as payment for their products and services. However, recipients are required to access the Internet, follow detailed instruction to retrieve their online certificate, and then are required to redeem the certificate at an online location, wherein a product is then shipped.

In an alternate embodiment of a conventional online gift certificate site, a buyer may purchase a "generic" gift certificate, which is then typically given as a gift to a recipient, whereby the generic gift certificate is supplied with a tracking number (which may be sent to a recipient, or may be e-mailed to the recipient?). The recipient may then log on to the gift certificate site, and "redeem" the generic gift certificate by selecting one or more specific gift certificates, which in sum are equal to the designated value of the original generic certificate. However, as with other online business which offer paper-based certificates for sale, the specific certificates are limited to an actual inventory of paper-based gift certificates which are available at that site. Upon redemption of the generic certificate, the specific certificate or certificates are then physically sent to the redeemer.

Another web-based company which sells gift certificates is located at "www.flooz.com", which enables an on-line buyer to purchase and send "on-line" currency, which is only available and usable on the Internet. When a buyer sends a recipient the "on-line" currency, such as by electronic mail, the recipient can then spend the "on-line" currency at one or more online sites which are registered to accept the "on-line" currency for online commerce.

In present embodiments of online commerce, buyers and sellers are linked electronically, at some point in the process, and merchandise (or redeemable paper-based certificates) are shipped to the buyer or alternate recipient, such as from a central warehouse linked to the seller. In such embodiments, there are inherent shipment costs, and there is often shipment delays.

On-line Ticketing Systems. In conventional networked commerce sites which offer tickets (*e.g.* such as for travel, sports, or entertainment), when a computer user purchases tickets online, a selling sites typically provides the buyer with a

serial number (*i.e.* such as a confirmation or tracking number, or even a general tick t number), such as through an e-mail notification. To receive the tickets, th buyer is then typically required to submit the confirmation or number at a will-call booth, whereby the submitted confirmation number is matched to the tickets (which may be previously printed, or may be printed upon redemption). If the submitted number is correctly matched to the tickets, the tickets are then given to the redeeming person. While such conventional online systems allow the online purchase of tickets, as well as the local pick-up of the purchased tickets, money is typically transferred upon the initial on-line acquisition of the tickets, and whereby anyone submitting the correct tracking number may be given the tickets. The single tracking number is confirmed off-line at the will-call booth and, is not authenticated with the on-line site.

The disclosed prior art systems and methodologies thus provide basic certificate systems, but fail to provide a secure certificate system in which allows issuers to create an virtual inventory of certificates, which may then be acquired online, and then redeemed locally. It would also be advantageous to provide a certificate system which allows customers to establish a private key that is unique to the transaction, which is subsequently used in a redemption transaction to authorize the local redemption with the online system. The development of such a certificate system would constitute a major technological advance.

SUMMARY OF THE INVENTION

A transaction network contains a networked certificate authority, by which one or more virtual certificates may be remotely defined and stored, such as by an issuer user through a issuer web portal interface. The virtual certificates correspond to a product or service denomination which is selected by the issuer, include a public key identifier. An acquirer user may locate and acquire one or more virtual certificates, through an acquirer web portal interface. When a virtual certificate is acquired by an acquirer, a corresponding private key is established by the acquirer, and is stored at the certificate authority in association with a record of the acquired certificate. As well, when the certificate is acquired, the acquirer typically submits payment agent information (*e.g.* such as credit card information). In one embodiment, funds are transferred during acquisition of the certificate. In a preferred embodiment, authorization for the transfer of funds occurs during the acquisition transaction. Certificate information is typically transferred to the acquirer,

or to an alt mat recipient, by which the holder of the certificat can redeem the certificate at a red mption location associated with an acquired certificat . The acquirer (or an alternate recipient of an acquired certificate to whom the acquirer has communicated the established private key), submits the certificate information at the redemption location, along with the established private key, to redeem the certificate. Upon communication of valid certificate information to the certificate authority , the redemption of the acquired certificate is authorized, while further use of the certificate is revoked.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a system block diagram of a transaction network for the issuance, acquisition and redemption of single-use certificates;

Figure 2 shows a single-use gift certificate;

Figure 3 is a schematic view of a single-use gift certificate identification packet;

Figure 4 shows a redemption process for a single-use gift certificate having an identification packet and an associated private key;

Figure 5 is a schematic block diagram of issuer facility options;

Figure 6 is a schematic block diagram of acquirer facility options;

Figure 7 is a schematic block diagram of transaction information data entry;

Figure 8 is a schematic block diagram of redeemer facility options;

Figure 9 shows the creation of virtual certificates by an issuer on at a certificate authority server;

Figure 10 shows an issuer virtual certificate creation module interface;

Figure 11 shows a graphic user interface for an issuer virtual certificate creation module;

Figure 12 is a block diagram of a virtual inventory stored within a database;

Figure 13 is a block diagram showing a site virtual inventory at an aggregate network site, and a search subset of the site virtual inventory directed by a search command at an acquirer terminal;

Figure 14 is a block diagram of an acquisition transaction module at an acquirer terminal, which is accessible from a selection of a virtual certificate from one or more alternate sites;

Figure 15 shows an embodiment of a partial certificate transaction network having a plurality of issuers, a plurality of acquirers, and a remote certificate authority; and

Figure 16 shows an embodiment of a partial certificate transaction network having a plurality of acquirer terminals, and an issuer terminal having a dedicated certificate authority.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a system block diagram of a transaction network 10 for the issuance, acquisition and redemption of single-use certificates 60 (FIG. 2). The transaction network 10 contains a networked certificate authority 12, through which one or more virtual certificates 60 are remotely created, such as by an issuer user ISR (FIG. 9), through issuer facilities 24 (*e.g.* such as through a web portal interface). The virtual certificates 60 typically correspond to a sellable commodity, such as a product or service denomination, which is selectable by the issuer user ISR. In an alternate embodiment, the virtual certificates 60 may correspond to a distributable commodity, such as a discount coupon for a product or service, or a reservation (*e.g.* such as for travel or dining), which is selectable by the issuer user ISR. Created virtual certificates 60 are stored on a database 18 which is associated with the networked certificate authority 12.

An acquirer user ACQ (FIG. 6), accessing the transaction network 10 through an acquirer terminal 26, may locate and acquire one or more virtual certificates 60, through an acquirer facilities 28 (*e.g.* such as through an acquirer web portal interface). When a virtual certificate 60 is acquired by an acquirer user ACQ, a corresponding private key 76 is established, either by the acquirer user ACQ, or

by the certificat authority 12, and is stored at th certificate authority 12 (*e.g.* such as within th database 18), in association with a record of th acquired certificat 60, along with other identifying information 98 for the acquired certificate 60.

As well, when a virtual certificate 60 is acquired, the acquirer user ACQ typically submits payment agent information 52 (*e.g.* such as credit card information). In one embodiment, funds are transferred during acquisition of the certificate 60. In a preferred embodiment, authorization for the subsequent transfer of funds occurs during the acquisition transaction 72. Certificate information 98 (FIG. 3) is typically transferred to the acquirer user ACQ, or to an alternate recipient RCP, by which the holder of the acquired certificate 60 can redeem the certificate 60 at a redemption location RL (FIG. 4,8) associated with an acquired certificate 60. The acquirer ACQ (or an alternate recipient RCP of an acquired certificate 60 to whom the acquirer user ACQ has communicated the established private key 76), submits the certificate information at the redemption location RL, along with the established private key 76, to redeem the certificate. Upon communication of valid certificate information to the certificate authority 12, the redemption of the acquired certificate 60 is authorized, while further use of the acquired certificate 60 is revoked.

Creation of Virtual Certificates. Figure 2 shows a single-use certificate 60, which may preferably be delivered in a printable form, either to an acquirer user ACQ, or to an alternate recipient RCP. A single-use certificate 60 typically includes one or more design elements 62, a denomination 64, one or more redemption rules 66, and identification information 74 (FIG. 3), which may include human readable information 68, and/or machine readable information 70 (*e.g.* such as a bar code symbol 70). An issuer user ISR 22 at an issuer terminal 22, in selective electronic communication with a certificate authority 12, has the means (*i.e.* issuer facilities) 24 to direct the certificate authority 12 to create one or more customized virtual certificates 60, for subsequent issuance to acquirer users ACQ at one or more acquirer terminals 26.

Establishment of Defined Virtual Certificates. Authorization for the construction of certificates typically occurs through an issuer facility 24, such as through a web portal 24 for a transaction network 10 operating across an internet 192, whereby an issuer user ISR (*e.g.* such as a merchant, or a product manager

for a plurality of stores RL) connects to the certificat authority 12 (*i.e.* such as through a certificate server portion 14 of a certificate authority 12).

The issuer user ISR defines detailed specifications for virtual single-use certificates 60 through a certificate specification interface 194 (FIG. 10), such as design specifications 62 and redemption rules 66, whereby the certificates 60 typically reflect sellable or distributable commodities, such as products and/or services which are available for pick up by a customer, typically at a redemption location RL (*e.g.* such as at a retail store, a distribution center, a box office, a ticket counter, or at a service provider).

An issuer user ISR 22 has the means 122 (FIG. 5) to control the modular design of one or more virtual certificates 60a-60n independently, either by selecting standard designs offered by the certificate authority 12, by uploading 122 one or more custom designs 62a-62n to the certificate authority 12, in the form of a computer file, or by specifying that a certificate 60 be issued using a combination of stock elements 162 uploaded through the issuer terminal 22. An issuer user may preferably incorporate the denomination 64 (*i.e.* a redemption value) of the certificate 60 as an additional element in the certificate identification packet 74. The denomination 64 typically corresponds to a product or service, or a selectable quantity of goods or services, which is to be received upon redemption of an acquired certificate 60. Additionally, an issuer user ISR may preferably incorporate an additional public key segment 82, as a part of the certificate identification packet 74, which may be used, for example, in mapping a certificate 60 to an issuer's coding scheme (*e.g.* such as to correspond to product serial numbers, part numbers, product color codes, product size, or service codes).

Storage of Virtual Certificates. Each virtual certificate 60 exists, until issued, as a virtual certificate 60 comprised of multiple independent textual elements 64,66 and/or graphical elements 62a-62n, which are stored by the certificate authority 12, in the secure database 18.

In one embodiment of the certificate system 10, the certificate authority 12 comprises two functional servers; a certificate server 14, as well as an authentication server 16. In alternate embodiments, a single certificate authority server 12 may perform both certificate establishment functions, as well as certificate redemption functions. In another alternate embodiment, the certificate

authority 12, the c rtificate module 14, th authentication module 16, and the certificate database 18 are integral modules within a certificate authority terminal 58 (FIG. 16).

Acquisition of Certificates and Establishment of Keys. Figure 3 is a schematic view of an acquisition transaction 72 for a single-use certificate 60. identification packet 74. During an acquisition transaction 72, an acquirer user ACQ typically provides a means to purchase a certificate 60, an authorization to purchase during a subsequent redemption transaction 104 (FIG. 4), or otherwise qualifies for issuance of the acquired certificate 60.

Certificate acquisition instructions are initially defined by an issuer user ISR at an issuer terminal 22, and are stored at the certificate authority 12, in association with each virtual certificate 60. Preceding an acquisition transaction 72, an acquirer user ACQ at an acquirer terminal 26, by means of the acquirer facilities 28, typically searches for or browses through a plurality of virtual certificates 60, (*i.e.* a virtual inventory). An acquirer user ACQ, upon selecting an acceptable virtual certificate 60, may selectably begin an acquisition transaction 72 to acquire the virtual certificate 60.

Before an acquisition transaction 72, a virtual certificate 60 to be acquired is constituted from the independent data elements 62,64,66 for the virtual certificate 60, which are stored in the secure database 18, for presentation to the acquirer user ACQ at an acquirer computer terminal 26 (*e.g.* such as in the form of an HTML document readable through acquirer facilities 28 by an internet browser application). As well, a stored virtual certificate 60 may represent the availability of one or more acquirable certificates 60, which is typically defined by an issuer user ISR, through selectable issuance restrictions 126 (FIG. 5,11).

Before an acquisition transaction 72, a virtual certificate 60 does not typically include established human readable information 68, and/or machine readable information 70 (*i.e.* the virtual certificate 60 is only a description of an acquired certificate, and may be used to represent one or more acquirable certificates 60). However, a virtual certificate 60 may include defined indicia 217,219 (FIG. 11), which identifies the placement and format of certificate information 68, 70 which is established upon acquisition. When a certificate 60 is acquired during an

acquisition transaction 72, th indep ndent data lements 62,64,66,68,70 ar thereaft r bound together within th databas 18.

During an acquisition transaction 72, in which the certificate authority 12 issues a certificate 60 to the acquirer user ACQ, a unique identifier 98 is bound to the issued certificate 60, typically comprising certificate information 74, which appears on the acquired certificate 60, which typically includes a denomination 64, and a public key 80 assigned by the certificate authority 12. In a preferred embodiment, the certificate information 74 includes a supplementary public key segment 82, which is assigned by an issuer user ISR. The certificate information 74 typically appears on the acquired certificate 60 through a printed number 68, or through other indicia, such as an encoded symbol, bar code, or three-dimensional bar code 70 (FIG. 2). Certificate information 74 which appears as human-readable information 68 or machine-readable information 70 on a printed acquired certificate 60 is preferably tamper-resistant. The unique certificate identifier 98 includes the elements associated with the certificate information 74, in combination with a private key 76, which is assigned to the certificate 60 as a part of the acquisition transaction 72.

The private key 76 is assigned to the certificate 60 at the time of acquisition, typically either by the acquirer user 92 or by the certificate authority 12. In embodiments in which the private key 76 is assigned to an acquired certificate 60 by the certificate authority 12, the private key 76 is typically generated randomly by the certificate authority 12, or is generated to comply with identification parameters selected 128 (FIG. 5) by an issuer user ISR. In embodiments in which the private key 76 is assigned to an acquired certificate 60 by the acquirer user ACQ, the private key 76 may be a unique private key 76 input by the acquirer user ACQ at he time of acquisition, or may alternately be a private key 76 which is used for one or more acquired certificates 60 for the acquirer user ACQ (*e.g.* such as a reusable "purchase PIN", or the acquirer's facility 28 access PIN).

The established private key 76 does not appear on the certificate 60, and is known only to the acquirer user ACQ, but is stored by the certificate authority 12, in association with the other data elements relating to the certificate 60, on the secure database 18.

Red mption of Certificat s. Figure 4 shows a red mption proc ss 90 for a single-use gift certificate 60 having a submitted identification pack t 98, which includes and an associated private key 76. The private key 76 must be provided to the redeemer 36 as part of the redemption process 90 by the acquirer user ACQ (FIG. 4), or by a third party and/or agent RCP to whom the acquirer ACQ has communicated the private key 76. A redemption clerk RC, such as a sales clerk, through a redeemer terminal 36, in communication with the certificate authority 12, by means of the redeemer facilities 38, or optionally, by means of a live operator intermediary 42, may authenticate a certificate 60, by providing the certificate authority 12 with the unique identification information 98 associated with the acquired certificate 60 (*i.e.* both the public keys 80,82 assigned to the certificate upon issuance, a denomination 64, as well as the unique private identification information 76 which is assigned to the certificate 60 upon acquisition (*i.e.* the private key 76).

In alternate embodiments of the certificate system 10, either the redemption clerk RC or the holder of the acquired certificate 60 can manually or automatically upload the certificate information 76 during a redemption process 90, such as through a point of sale terminal 40. As well, either the redemption clerk RC or the holder of the acquired certificate 60 can enter the private key PIN 76 into a point of sale terminal 40. One or more redeemer terminals 36, point of sale terminals 40, and/or telephonic devices 40 may be located at the redemption location RL, and may include a variety wireless network communications, such as a localized wireless network at the redemption location RL, or as remote wireless connections across a network 192 (FIG. 9) to the certificate authority 12.

Authorization of Certificate During Redemption. The certificate authority 12 authenticates a certificate 60, on the basis of the certificate identification packet 74 (which includes the public key 80 and supplementary public key 82), and the private key 76 submitted by a redemption clerk RC, such as through redemption terminal 36 (or alternately, by the holder ACQ,RCP of the certificate 60, such as directly into a point of sale terminal 40). As seen in comparison step 100 in Figure 4, the certificate authority 12 queries the secure database 18, which stores the independent elements associated with the acquired certificate 60, to determine whether the certificate identification packet 74 and the private key 76 originally associated with the certificate 60 upon issuance matches the certificate identification packet 74 and private key 76 identification information provided to

the certificate authority 12 through the redeemer facilities 38, as shown in matching step 102. If the unique id ntification sets correlate 103, the certificate authority 12 validat s the certificat 60, and upon instructions by the red mption clerk RC, authorizes the redemption transaction 104. If the unique identification sets do not correlate 105, the certificate authority 12 typically cancels 106 the redemption transaction 104, either by requesting that the acquirer ACQ resubmit the certificate information 74 and the private key 76, or by revoking the certificate 60 (*e.g.* such as if the certificate 60 has previously been marked as used).

Authorized Redemption Transaction and Cancellation of Single-Use Certificate. Upon a successful authorization transaction 104 of an acquired certificate 60, the certificate authority 12 allows the redemption clerk RC to proceed with redemption of the certificate 60, and revokes the single-use certificate 60 (*i.e.* thus preventing further use of the certificate information 74,76). The certificate authority 12 revokes the acquired certificate 60 by updating the certificate information stored on the secure database 18 (*e.g.* by marking the acquired certificate as "used"). In one embodiment of the certificate system 10, the certificate authority 12, by means of certificate payment facilities 48, initiates the transfer of payments between the parties of the acquisition transaction 76 and the redemption transaction 104, by issuing transfer instructions to the certificate payment agent 58, the acquirer payment agent 52, the issuer payment agent 54, and the redeemer payment agent 56.

When a redemption transaction 104 is successfully authorized by the certificate authority 12, the certificate authority 12 preferably downloads a transaction code 181 (FIG. 8) to the redemption terminal 36, which preferably becomes part of a redemption record 41 (FIG. 1) by the redemption location RL, and is also preferably transferred to the acquirer user ACQ or alternate recipient RCP (*e.g.* such as within a redemption receipt 41).

Virtual Certificate Creation Options. Figure 5 is a schematic block diagram 100 of issuer facility options, which includes initial registration of new issuers 112, secure entry 114 into the transaction network 10, an issuer certificate parameter module, and an issuer report module 116.

Registration of Issuers. An issuer ISR who is not previously registered as a client with the certificate authority 12 is preferably guided through a registration

process 112, during which th issuer user is required to input relevant information (*e.g.* such as the nam of the issu r us r, the business name, one or mor redemption locations RL, as well as relevant banking information). The preferred registration of issuers allows the certificate authority 12 to confirm that the issuer is a legitimate entity (*i.e.* such as an existing, valid business), and that the issuer is offering real goods and services. As well, the preferred registration process 112 includes the input of banking information related to issuers (*e.g.* such as issuer payment agent 54 information), whereby funds may be properly transferred to issuers, from acquirers, such as when an acquired certificate 60 is redeemed at a redemption location RL.

The registration process 112 also typically includes a registration validation step, by which the certificate authority 12 or other independent entity checks pertinent registration information, such as bank account information, credit references, or merchant identification number. Based upon a successful registration step 112 and validation step, the certificate authority 12 preferably assigns an access number 113 to the new issuer, and sends the a registration notification and access number 113 to the new issuer (*e.g.* such as by an e-mail notification). In an alternate embodiment, a new issuer ISR, having submitted a valid merchant number at registration step 112, may automatically gain an access number 113 and subsequent access to the certificate authority.

Issuer Access. When an issuer user ISR is properly registered with the certificate authority 12, the issuer user ISR may gain ongoing access to the certificate authority 12. A registered issuer user ISR typically inputs the previously established unique issuer access code 113, to log 114 onto the certificate authority 12.

Creation of Certificate Parameters. An issuer user ISR at an issuer terminal 22, in secure communication with the certificate authority 12 (*e.g.* such as through initial registration 112 or a subsequent log on process 114), by means of issuer facilities 24 (*e.g.* such as through a web portal), can direct a large variety of certificate parameters 115. While an issuer user ISR may direct the creation of virtual certificates 60 through the selection of standard certificate elements 62, 64, 66, the issuer user ISR may optionally upload discrete data elements 62-70 to the certificate authority 12, which are unique to the issuer ISR, for storage as stored elements associated with one or more virtual certificates 60, or may

oth rwise dir ct certificate param ters, at step 115, by selection of options off red by the c rtificate authority 12.

At issuer information selection step 118, the issuer preferably selects or uploads issuer information 118, such as company information, or promotional information. Issuer information 118 may be preferably included within a virtual certificate 60, or may be included as information at a network site offering selection of the appropriate certificate 60. For example, a web page which includes a selectable certificate for a business typically includes other issuer information 118 to describe the business, or to describe the selectable commodity, such as a product or service description.

At denomination selection step 120, the issuer preferably selects or uploads denomination parameters for a virtual certificate 60. The denomination 78 may be in the form of a currency denomination, or in the form of a code associated with a product, a service, a coupon, a voucher, or other instrument for which the an acquired certificate 60 may be redeemed. The issuer may preferably authorize 120 the certificate authority 12 to issue certificates 60 within a set range of selectable denominations, or authorize the creation of virtual certificates 60 with a value determined by an acquirer user ACQ.

Examples of virtual certificates 60 that can be offered to acquirers by the certificate authority 12 on behalf of issuers include certificates denominated as full payment in exchange for an item and/or service (*e.g.* such as a gift certificate which is redeemable for an item and/or service, or a ticket or coupon voucher redeemable for an actual ticket), certificates 60 which may be redeemed as partial payment for a particular item or service, denominated as a currency amount (*e.g.* such as a gift certificate denominated in a currency amount); or a certificate 60 redeemable for currency, denominated in a currency amount (*e.g.* such as a "traveler's check").

At issuer artwork selection step 122, the issuer preferably selects or uploads artwork graphics 62a-62n which may be unique to the issuer (*e.g.* such as logos, trademarks, or other artwork, such as borders, illustrations, or photographs). The artwork graphics 62a-62n to be uploaded are typically uploaded in the form of graphics files 62a-62n (FIG. 2)(*e.g.* such as in TIFF, JPEG, PICT or EPSF file formats), which are associated with an issuer ISR, a redemption location RL, a

product or service, or basic certificate artwork 62. In a preferred embodiment of the artwork selection step 122, the issuer user ISR may upload all or part of a certificate design layout, such as defined within page layout software (*e.g.* such as through the use of PAGEMAKER™, by Adobe Systems, Incorporated, of San Jose, CA, or through xPRESS™, by QUARK, Inc.), or transferred through a portable document format (PDF) (*e.g.* such as through the use of ACROBAT™, by Adobe Systems, Incorporated, of San Jose, CA). As well, an issuer user may preferably define or control the use of fonts and typefaces to be used, within the artwork selection step 122.

At redemption rule information selection step 124, the issuer preferably selects or uploads redemption rules 66, such as an expiration date, any exclusion of redemption on the basis of geographic location, or other redemption rules 66 unique to the issuer. As seen in Figure 2, redemption rule information 66 may be included as printed information on an acquired certificate 60.

At issuance restriction information selection step 126, the issuer preferably selects or uploads issuance restrictions to the certificate authority 12, such as to limit the number of acquired certificates 60a-60n to be issued by the certificate authority 12 on behalf of the issuer 22, such as within a specified time frame, within a geographic region, or on the basis if other criteria unique to the issuer. For example, since a virtual certificate 60 may represent one or more acquired certificates 60, the issuer may preferably select or upload the availability of acquired certificates 60 for one or more redemption locations RL. As well, as a real inventory of goods or services changes at one or more redemption locations RL, the issuer user ISR may preferably update the selected availability of acquirable certificates 60.

At issuance certificate identification parameter selection step 128, the issuer preferably selects or specifies the format of unique certificate supplementary public key identification 82 (FIGS. 3,4). For example, the issuer may require unique certificate public key identification 82 which corresponds to existing product codes, inventory, or existing issuer certificate systems. Therefore, the issuer may optionally select, enter or upload certificate identification supplementary public key parameters 82, to be combined with certificate identification public key information 80 (FIG. 3) assigned by the certificate authority 12. As well, in a preferred embodiment of the certificate identification

param ter sel ction step 128, the issuer user ISR may select the format used by th certificate authority 76 to establish private keys 76, or to guide the input of private keys 76 by an acquirer user ACQ, during an acquisition transaction 72.

Issuer Reports. If an issuer user ISR has already created certificates 60, the issuer user ISR, through the report interface 116, can view, print, or download reports based upon previously created virtual certificates 60, acquired certificates, or for redeemed certificates 60. An issuer user ISR, at an issuer computer 22, is preferably provided with report options 116 to request, view, print, or download, in near real time, various reports relating to certificate parameters, issuance, redemption, and other information.

For example, at certificate review step 130, an issuer may preferably review existing parameters and data elements associated with a virtual certificate 60 or a series of virtual certificates 60a-60n. At issued certificate review step 132, an issuer may preferably review, print, or download information regarding issued certificates. At redeemed certificate review step 134, an issuer may preferably review information regarding certificates 60 which have been redeemed and/or revoked.

Acquirer Options. Figure 6 is a schematic block diagram 140 of acquirer facility options. An acquirer user ACQ at an acquirer terminal 26, through acquirer facilities 28, establishes a secure communication with the certificate authority 12, such as through a registration 142 or logon step 145. An acquirer user ACQ who is not previously registered 141 as a buyer/client with the certificate authority 12 is preferably guided through a registration process 142, during which the acquirer user ACQ is may preferably be required to input relevant acquirer information (*e.g.* such as the name of the acquirer user, product or service preferences, and selectable redemption regions). The preferred registration 142 of acquirer users ACQ allows the certificate authority 12 to guide the acquirer to real goods and services.

Based upon a successful registration step 142, the certificate authority 12 preferably assigns an acquirer access code 143 to the new acquirer ACQ, or alternately allows the acquirer user to designate the acquirer access code 143.

Acquirer Access. When an acquirer user ACQ is properly registered with the certificate authority 12, the acquirer user ACQ may gain ongoing access to the certificate authority 12. A registered acquirer user ACQ typically inputs the previously established unique acquirer access code 143, to log 144 onto the certificate authority 12.

The acquirer user ACQ is then typically presented with certificate acquisition options 145, such as the means to browse through or search 148 for virtual certificates 60 (to be assembled from the discrete elements) stored on the database 18 by a certificate authority 12, and to direct various parameters 145 regarding issuance of one or more certificates 60. For a virtual certificate 60 which an acquirer user ACQ proceeds to acquire, the acquirer user ACQ enters transaction information at transaction step 150. In a preferred embodiment of the acquirer facilities 28, the input acquirer payment agent information 52 is securely stored, either during the acquirer registration process 142 or during a certificate transaction step 150, whereby the transaction information may be retrieved and selectably reused for the acquisition of one or more certificates 60 (*e.g.* such as through an acquisition "quick" menu, which allows a subsequent acquisition transaction 72 to use credit information which was previously entered).

For previously acquired certificates 60 which have not been redeemed, the acquirer may preferably be able to cancel the certificate 60, at cancellation step 151. As well, for previously acquired certificates 60 which have not been redeemed, the acquirer user may preferably request a replacement for a certificate (*e.g.* such as for a lost or destroyed certificate). At customization step 153, the acquirer user ACQ may preferably be given customization choices, such as integrating an acquired certificate 60 within a printed card, or modifying the artwork to display other information (*e.g.* such as the name of an alternate recipient RCP). In addition, for previously acquired certificates 60 which have not been redeemed, an acquirer user ACQ may access reports, at step 146, regarding acquired certificates. For example, at redemption location report step 154, an acquirer user may view, print, or download a list of alternate redemption locations RL, or supplementary information regarding the redemption locations RL (*e.g.* such as a map), for an acquired certificate 60.

Certificate Acquisition and Input of Acquirer Information. Figure 7 shows a detailed acquisition transaction process 150, by which an acquirer user may

direct a certificat authority 12 to issue on or more selected certificates 60a-60n from an inventory of available virtual certificates 60. An acquirer typically receives an issued certificate 60, in exchange for an authorization to charge the acquirer upon certificate redemption, for payment at the time of acquisition, or on the basis of other acquirer qualifications. An acquirer may upload other necessary instructions and transaction information 162 to the certificate authority 12, which are then stored (*e.g.* such as in database 18) as additional independent elements associated with the issued certificate 60. Acquirer entered transaction information 162 typically includes name and address information 164, credit card or other information 166 associated with the acquirer's payment agent 52, assignment 170 by the acquirer of the secret private key 76 (FIG. 3) to be associated with the selected certificate 60, and a selected delivery method 172 for the certificate 60. As described above, the private key 76 is established in relation with an acquired certificate 60 at the time a certificate 60 is acquired, whereby the private key 76 is established by the certificate authority 12, or is entered by the acquirer user ACQ.

For a private key 76 which is established by the acquirer user ACQ, the private key 76 may be unique to a single transaction 72. As well, the acquirer user ACQ may alternately establish a private "acquisition" key 76, which may be associated with one or more acquisition transactions 72. Furthermore, the acquirer user ACQ may alternately use the established acquirer registration key 142 as a private key 76, which is then associated with one or more acquisition transactions 72.

The acquirer is typically prompted (*e.g.* such as by a required data entry field or a dialog box) to input the private key 76 (*e.g.* such as a personal identification number (PIN) into the system. The acquirer is preferably prompted to enter the private key 76 twice, to verify that the acquirer user has correctly entered a known private key), to be stored in association with the certificate 60. In a preferred embodiment of the certificate system 10, an acquirer may specify that the private key 76 to be associated with an issued certificate 60 be comprised of other identification information associated with the transaction, such as an account number which associates the acquirer with the acquirer's payment agent 52 (*e.g.* a credit card number), or a debit card number. As well, an acquirer user ACQ may preferably select and/or specify a denomination 168 for an acquired certificate 60 (*e.g.* such as a currency amount), typically by selecting from among denominations presented by an issuer. In a preferred embodiment of the

certificate system 10, the certificate authority 12 sends a confirming e-mail to the acquirer.

When the acquisition of a certificate 60 is complete, the certificate authority 12 preferably allows the acquirer user ACQ to preview a printable version of the certificate 60, and typically presents certificate delivery options 172 to the acquirer user ACQ, such as the transfer of a downloadable PDF file to the acquirer terminal 26, the e-mail of certificate information 98 to the acquirer terminal 26 (or to an alternate recipient RCP), the facsimile transmission 32 of an acquired certificate 60, an electronic encoding 34 of a smart-card based certificate, or the electronic transfer of the acquired certificate 60 to a redeemer computer 36 at a desired redemption location RL.

The acquirer user ACQ can preferably send an e-mail or other message to an alternate recipient RCP (*e.g.* such as for a gift certificate), directing the recipient RCP to log on and pick up the certificate, either for printing, such as at the recipient's computer, at the redemption location RL, or at a third party (*e.g.* such as at a third party mail service provider). If no hard-copy of the acquired certificate 60 is desired, or if printing is not feasible, the certificate information can be transferred directly to the issuer merchant's computer (*e.g.* a paperless electronic certificate), by which the acquirer ACQ or alternate recipient RCP need only to visit a redemption location RL, and supply the private key PIN number 76 to the redemption clerk RC.

Examples of alternate delivery methods for an acquired certificate 60 which may be specified by an acquirer ACQ include downloading of the certificate 60 as an electronic file (*e.g.* such as within a portable document format (PDF) file (by ACROBAT™, of Adobe Systems, Inc., of San Jose California), or as an electronic description transferred via the acquirer's computer 26 to a transaction card encoder 34, or for printing on a printer 30 connected to the acquirer's computer 26, or for subsequent printing later by the acquirer user ACQ.

A redeemer (*i.e.* a store clerk) typically needs only the certificate information 74 (which includes the denomination 78 of the certificate 60 and public keys 80,82), in combination with the acquirer's private key 76, to validate an acquired certificate 60. Hence, an issuer may request that a certificate 60 be delivered in the form of an e-mail, containing only these items, or as encodeable "smart card" data that can

b magn tically stored by the acquirer using a "smart card" ncoder 34 attached to the acquirer computer 26 or other communication device.

An alternate preferred delivery option 172 which an acquirer may specify is that an acquired certificate be printed by the certificate authority 12, and delivered by a postal service or other delivery service, to an address specified by the acquirer user ACQ (the typically the address of the acquirer ACQ, or the address of an alternate recipient RCP, such as if the acquired certificate 60 is intended as a gift certificate).

Another alternate preferred delivery option 172 which an acquirer may specify is that an image (*e.g.* such as a TIFF file) of an acquired certificate 60 be faxed by the certificate authority 12, to a facsimile (fax) machine designated by the acquirer user ACQ (typically a facsimile machine 32 associated with the acquirer ACQ, or a fax machine 32 associated with an alternate recipient RCP).

As seen in Figure 6, until an acquired certificate is redeemed, an acquirer preferably has the ability to cancel 152 a previously acquired certificate 60, or to request that an acquired certificate be revoked and replaced 153 by a new certificate 60. For example, if an acquirer user accidentally damages, destroys, or loses a previously printed acquired certificate 60, the acquirer may simply print out a new certificate 60, or have a new certificate delivered or faxed, and may either retain the previously stored private key 76, or may specify a new private key 76.

Since an acquired certificate 60 may only be used for redemption once (at which time further use is revoked), there is no financial risk to the issuer ISR in the use of replacement certificates 60, or that a downloaded certificate 60 be printed more than once. As well, even if a certificate is lost and retrieved by a second party, or is stolen, the lost acquired certificate is unredeemable, without submittal of the private key 76, which is not included as printed information on a certificate 60.

As shown in Figure 6, an acquirer is preferably allowed to query the secure database 18 for available redemption locations 154 for an acquired certificate 60, typically on the basis of a geographic screening. The acquirer may request redemption locations 154 when the certificate is acquired, and is preferably provided with ongoing access to redemption locations 154 (such as if an alternate

redemption location is desir d, and is allowed by the redemption rules 66 for an acquired certificat 60.

Prior to acquisition, the virtual certificate 60 is merely a defined product or service, associated with an authorization to produce a certificate, as defined by an issuer, for the defined product or service. However, after the acquisition transaction 72 is completed, the certificate 60 then exists as an established entity within the database 18, thereby becoming a token which directly corresponds to the corresponding defined product or service, which is to be surrendered by the seller to the holder of the certificate 60 at the time of a completed redemption transaction 104.

In addition to the previously defined public keys 80,82 and private key identifiers, upon issuance of an acquired certificate, the certificate authority 12 preferably creates or assigns a unique issued certificate number (*e.g.* such as certificate "XYZ-203-4067") which corresponds to the acquired certificate 60, as well as to the collection of the defined elements of the certificate 60 (*e.g.* such as the associated graphics 62, redemption rules 66, and denomination 78), which are bound within the database 18 after the acquisition transaction.

In a preferred embodiment, the certificate authority 12 communicates the acquisition transaction 72 to the issuer (*e.g.* such as through issued certificate reports 132), such that the product or service which is to be received upon redemption may be held (*i.e.* reserved). For a product within an inventory at a redemption location, the product may preferably be placed on hold. For a designated service, the issuer may preferably use the acquisition information to schedule personnel or equipment, or to limit the further sale of goods or services (*e.g.* such as for an airline flight, which has a limited number of seats available for a scheduled flight and time).

Before the acquisition transaction 72, the virtual certificate 60 is merely an authorization to construct a certificate 60, wherein the virtual certificate 60 is typically stored as a product or service category within a virtual inventory of other virtual certificates. If a certificate is never acquired, there is no effect upon a real inventory. If an inventory of real goods an services (or associated cost structures) change for an issuer, they may simply reaccess the certificate system 10, and

remove or edit previously defined virtual certificates 60, or create other certificat s 60 which reflect their current goods, services, or cost structures.

For example, for an issuer/merchant who has a limited number of products available (*e.g.* such as three mission-style coffee tables), the issuer ISR would preferably limit the availability of virtual certificates 60, as an issuance restriction at issuance restriction step 126 (FIG. 5). If an acquirer user ACQ acquires a certificate for such a commodity having a limited availability, the certificate authority 12 preferably limits the acquisition to the defined virtual inventory. As well, for an issuer ISR which creates virtual certificates 60 for a plurality of redemption locations RL, the issuer may preferably create virtual certificates 60 which are unique to one or more of the redemption locations. For example, a first redemption location RL may sell products which ar not available at a second similar redemption location RL, or the selling price for a product may be different at different redemption locations RL. For virtual certificates 60 which are defined as virtual coupons (*e.g.* such as for a discount at a redemption location RL), an issuer can preferably define different discount rates for different redemption locations RL.

Certificate Redemption. Figure 8 is a detailed schematic block diagram 174 of redeemer facility options. A redemption clerk RC (*e.g.* such as a sales clerk at a redemption location), establishes electronic communication with a certificate authority 12 through redeemer facilities 38. As seen in Figure 1, the redeemer facilities 38 are typically accessed through a redeemer computer terminal 36, a redeemer POS terminal 40, or by a telephone 44 (either by using a keypad driven menu, or through a live operator intermediary 14). One or more redeemer terminals 36, point of sale terminals 40, and/or telephonic devices 40 may be located at the redemption location RL, and may include a variety wireless network communications, such as a localized wireless network at the redemption location RL, or as remote wireless connections across a network 192 (FIG. 9) to the certificate authority 12, such as to the authorization server 16.

When an acquirer user ACQ (or alternate recipient RCP) desires to proceed with a redemption transaction 90 at a redemption location, the acquirer user ACQ typically hands the printed certificate 60 to a redemption clerk RC, and communicates the private key 76. The redemption clerk RC then validates the issued certificate 60, to obtain a redemption authorization code 181 from a

certificate authority 12 to redeem the certificate 60, thereby performing a certificate authentication 178. In a preferred embodiment of the certificate system, the acquired certificate includes redemption instructions 66 (*i.e.* terms of service instructions), which a redemption clerk RC preferably follows to redeem the acquired certificate 60. The redemption clerk RC uploads 180 certificate information 98 to the certificate authority 12, which typically includes the certificate denomination 78, the public keys 80,82, as well as the private key 76 (which is submitted separately by the acquirer user ACQ).

In a preferred embodiment of the certificate system 10, communication of redemption information 98 (*e.g.* such as communication of the required public keys 80,82, private key 76 and denomination 78) of the certificate 60 to the certificate authority 12 is made by an electronic link 39 with a point-of-sale (POS) terminal 40 and/or a card code scanner 40, a redeemer computer 36, or by other means having the ability to establish an electronic link 39 with the certificate authority 12. For example, a redemption clerk RC preferably uses a bar code image scanner or other POS terminal 40 to determine the redemption information 98, while the acquirer ACQ typically enters the private key 76 (*e.g.* such as a PIN number) into a keypad of a POS terminal 40.

In a redemption system 174 which comprises a telephone terminal 44, the communication of the redemption information 98 of the certificate 60 to the certificate authority 12 may be made using a touch-tone telephone keypad on the telephone 44, or by live-phone contact to an operator intermediary 45 in communication with the certificate authority 12.

Authorization of Certificate Redemption. Upon authentication of the certificate by the certificate authority 12, on the basis of a correlation of the unique certificate identification 74 in combination with the acquirer's private key PIN 76 with the transaction records associated with the certificate 60 stored in the secure database 18, the certificate authority 12 authorizes the redemption, and revokes further use of the acquired certificate 60.

In a preferred embodiment of the certificate system 10, upon authentication of a certificate 60, the certificate authority 12, creates a unique redemption transaction code 181, which through redeemer facilities 38 may be downloaded 182 or otherwise communicated to a redemption terminal 36,40,44. The certificate

authority 12 preferably stores th redemption transaction code 181 in association with th data elements relating to the certificat 60. The redemption transaction code 181 may subsequently be used by redeemer personnel RC, such as through a redemption terminal 36, to authenticate to the certificate authority 12 that the redemption of the certificate 60 occurred, in the event there are subsequent discrepancies in the final financial reconciliation of payment transfers associated with the redemption transaction 104.

The certificate authority 12 has the means 46 to selectively establish an electronic communication link 57 with an acquirer payment agent 52, to request payment, and transmits to the acquirer payment agent 52 the identification needed by the acquirer payment agent 52 to authenticate the acquirer user ACQ, and obtain approval for the redemption transaction 104.

Therefore, upon a successful redemption transaction 104, the certificate authority 12 typically manages the transfer of funds between appropriate payment agents. In one embodiment the certificate authority 12 sends instructions to the authority payment agent 58, to transfer funds to the redeemer payment agent 56 of a redeemer.

Issuer Creation Module. Figure 9 shows the creation of a virtual certificate 60 by an issuer user ISR at an issuer terminal 22, through issuer facilities 24. As described above, an issuer user ISR, in communication with the certificate authority 12 across a network 192 (*e.g.* such as the internet), typically through a certificate server 14, can direct the creation of one or more virtual certificates 60. The issuer facilities preferably include a issuer certificate creation module 194, in which the issuer may define attributes for a virtual certificate 60, such as denomination information 64a,64b, certificate design information 62a-62n, redemption rules 66a-66n, and issuer defined supplementary public key information 82.

Figure 10 shows an issuer virtual certificate creation module interface 194a, which preferably includes an issuer information module 196, an issuer commodity denomination module 198, an issuer design module 200, and a redemption rule module 202.

The information module 196 typically includes issuer business name 204a, issuer address 204b, registration information 204c, issuer description copy 204d, and a comprehensive list 204n of all associated redemption locations RL. The commodity denomination module 198 typically includes commodity type 206a, commodity category 206b, and a denomination descriptor 206c. Other denomination attributes may be set with denomination attribute control 206d.

The issuer design module 200 typically includes selection of various design element 62, such as through add design element control 122a, design library control 122b, and upload design control 122c. Attributes for a design are preferably set by attribute control 208. A design element 62 is preferably activated by control 210. A design element 62 which is not needed may be deleted by deletion control 212. The issuer design module 200 preferably includes indicia selection control 122d, in which the issuer user may define the number and type of certificate identification indicia 88 (FIG. 3) to be displayed on an acquired certificate 60, such as a human-readable serial code 68, or machine readable indicia 70. The redemption rule module 202 typically includes user selectable expiration limitations 124a, location selection 124b, or other redemption rules 124c. As well, other issuer entered restrictions may be entered, such as availability 126a, or other restrictions 126n.

Figure 11 shows a preferred graphic user certificate layout interface 194b for an issuer virtual certificate creation module 194. The certificate layout interface 194b preferably includes a work area 214, in which an issuer user ISR can establish a defined layout for virtual certificates 60, as they may appear on a network site, or as an acquired certificate 60 may look if a printable form is used. User selectable elements, such as denomination 64, design elements 62a-62n, redemption rules 66, or issuer defined certificate identification elements 82, preferably appear as selectable icons. The selectable elements are preferably established in the issuer virtual certificate creation module interface 194a, such that selectable elements are preferably limited to the defined attributes. Certificate identification control 128 allows an issuer user ISR to control the placement of certificate identification human readable indicia 217 and/or machine readable 219, wherein certificate information 68, 70 is established and located upon acquisition. When a certificate 60 is acquired during an acquisition transaction 72, the independent data elements 62,64,66,68,70 are thereafter bound together within the database 18.

The work area 214 preferably allows the issuer user ISR to create a certificate layout in a WYSIWYG work nvironment, wh rein elem nts may b "dragged into position in the area, and wherein a certificate preview 216 (*e.g.* such as a thumbnail or full size image) is created within the work area 214. An issuer user may save 218 a virtual certificate 60, rename 220 a certificate as a new certificate 60, print 222 a proof copy, or be guided 224 to context-sensitive help screens.

Creation of Inventory. Figure 12 is a block diagram 226 of a virtual inventory 228 stored within a database 18. Each created virtual certificate 60 is a defined collection of elements, such as denomination elements 64a,64b, redemption rules 66, such as applicable redemption locations RL, and a public key identification packet 80,82. One or more virtual certificates 60, which are stored within the database 18, become a virtual inventory 228 of goods and services, which can then be accessed through one or more network locations (*e.g.* such as through web sites).

The virtual inventory 228 typically comprises a wide variety of goods and services. As well, the virtual inventory 228 typically comprises virtual certificates which may be redeemed within different geographic regions. For example, a first inventory subset 230a within the virtual inventory 228 may be a subset of similar products or services, but with no limitation of a redemption location RL. By contrast, a second inventory subset 230b within the virtual inventory 228 may be a subset of all products or services which may be acquired, but within a small geographic region.

Certificate elements, such as commodity type, denomination, product descriptors, and redemption locations RL are preferably searchable data elements, by which virtual certificates 60 for products or services may be quickly located.

One or more network sites, such as aggregate sites 234 (FIG. 13), may preferably be established, to allow an acquirer shopper ACQ to locate an appropriate subset 230 of virtual inventory 228, such as to allow for the sale of similar goods and services from a plurality of issuers ISR, or to allow the acquisition of certificates of goods and services which can be redeemed within a given region (*e.g.* such as within a town, postal region, county, or state). As well, from a site 234 having a subset 230 of any portion of the virtual inventory, the

acquirer user ACQ is preferably provided with search tools 238 by which appropriate virtual certificates 60 are located.

Figure 13 is a block diagram showing a site virtual inventory 236 at an aggregate network site 234, and a search subset 240 of the site virtual inventory 236 directed by a search command 238 within a browsing (*i.e.* shopping) module 148 at an acquirer terminal 26n.

In a preferred embodiment of the certificate system, an acquirer user ACQ is able to control (*e.g.* such as by search command 238) which of the available virtual certificates 60 are to be displayed, on the basis of a particular store or brand of product, or on the basis of certificate types and/or issuer types categorized by one or more descriptive criteria available in the discrete information associated with each unissued virtual certificate.

In a preferred embodiment of the certificate system 10, an acquirer user ACQ may specify a geographic location for a desired redemption location RL (*e.g.* such as a redemption within a postal code area or telephone area code region). The certificate authority 12 uses the selected geographic descriptor to create a subset 240 of available virtual certificates 60, such that only redeemable certificates associated with the specified geographic location are presented to the acquirer user ACQ. For example, an issuer ISR may have specified geographic exclusions for a certificate which correlate to the acquirer's geographic identification information, precluding redemption within the acquirer's geographic area.

Therefore, an acquirer user ACQ can readily locate redemption locations RL for one or more products or services which are available as selectable virtual certificates 60. Upon initiating a search, such as by product type, service type, zip code, town, or state, the certificate authority 12 preferably presents a browseable subset 240 of the entire virtual inventory 228 (or of an aggregate inventory 236), which matches search limiters entered by the acquirer user ACQ.

For example, an acquirer user in Figure 13 may have entered "coffee" as a search descriptor at an aggregate site 234, within a zip code of "97213", with a selected local radius of 25 miles. The certificate authority 12 would then perform a search for product types or description text that includes the word "coffee", for virtual certificates 60 which include a one or more redemption locations within the

"97213" zip code (as well, in this preferred embodim nt, within a region roughly defined by a 25 mile radius from the center of the "97213" area cod). In this manner, the acquirer user may be presented with a selection of virtual certificates 60 which match the entered search criteria.

Since the inventory 228 of virtual products and services is a virtual product inventory 228, one or more of the virtual products or services may be accessed by a plurality of network locations 234. For example, a virtual certificate 60 created by an issuer ISR who sells computers may correspond to the acquisition of a small, hand-held tape recorder. The corresponding virtual certificate 60 may be advantageously listed within a plurality of aggregate sites 234, such as an aggregated site 234a for electronics, an aggregated site for business supplies 234b, an aggregated site for school supplies 234c, or even a site for gadgets or gifts 234d.

From an aggregated web site 234, which offers virtual certificates 60 for goods or services from a plurality of businesses ISR, RL, an acquirer user ACQ, searching or browsing through an aggregate inventory 236 of virtual certificates 60, is preferably guided to web pages or sections of web pages 248 (FIG. 14), which describe one or more certificates 60, along with a presentation of other information 251a,251b which was input by the user to be displayed with the virtual certificate 60 (*e.g.* such as a store or product logo, a description of the store, business address, phone number, or map, a description of the product or service represented by the virtual coupon 60, or even recorded audio or video information). In a preferred embodiment, the displayed information 251 may include review information, such input by prior customers. In addition, links to related virtual coupons for other products and services from the same issuer may preferably be included within the description screen 248.

As well, the same certificate 60 may be accessed from the issuer/merchant's own network site 242, which has a site virtual inventory 236 limited to virtual certificates 60 that are created by the issuer ISR. For example, a merchant site 242 (*i.e.* such as an issuer/redeemer site) that is established by a merchant may include a wide variety of information 244, typically related to the issuer ISR or associated redemption locations RL. Within the merchant site 242, the issuer ISR may preferably provide direct access to virtual certificates, such as through selectable certificate icons 246 (FIG. 14).

Upon selection of a selectable certificate locator icon 246, an abbreviated certificate description page 248 is typically presented to the acquirer user ACQ at the acquirer terminal 26, which describes the goods and services for the selected virtual certificate 60. The certificate description page 248 provides a virtual "shelf space", which may be accessed from one or more aggregate sites 234, or from a merchant web site 242. The certificate description page 248 typically provides issuer defined options, such as headers, product or service descriptions, including selectable options to view and selectably acquire 250 coupons or certificates.

An acquirer user ACQ therefore may preferably access the inventory 228,236 of virtual certificates 60 through both one or more larger aggregated sites 234, as well as through existing merchant sites 242. An acquirer customer ACQ typically finds a virtual certificate 60, or does a search to find various network sites offering virtual certificates 60 for desired goods or services.

Acquisition Transaction Module. Figure 14 is a block diagram 241 of acquirer access to an acquisition transaction module 252, wherein the acquisition transaction module 252 is accessible through one or more aggregated sites 234, as well as through an existing merchant site 242.

Selection of a selectable acquisition icon 250 by an acquirer user ACQ typically transfers the acquirer user ACQ to a acquisition transaction module 252 within the acquirer facilities 28 for the certificate system 10. While the acquisition transaction module 252 is operated within the certificate system 10, the description of the selected available product or service, the denomination 64 for the selected available product or service, as well as other redemption rules 66, are determined by the issuer options 114 (FIG. 5). As well, limitations on appropriate acquirer payment agents 52 are initially selectable 252 by the issuer, and limit the payment agent choices within the shopping transaction module 252.

For example, if a redemption location RL for an issuer ISR accepts VISA™ or AMERICAN EXPRESS™ credit card payment agents 52, but does not accept MASTERCARD™ credit card payment agents 52, the issuer ISR preferably limits the selectable 256 payment agents 52, to be displayed and selectable

within the shopping transaction modul 252, to VISA™ or AMERICAN EXPRESS™ payment agents 52.

While the shopping transaction module 252 is typically used for a single acquisition transaction 90, related to a single issuer ISR, the shopping transaction module 252 can alternately be used to acquire one or more certificates related to the same issuer ISR, for a single redemption location RL. Details of the acquisition transaction are displayed within the transaction invoice 254.

As described above, during an acquisition transaction 72, the acquirer facilities 28 typically prompt the acquirer user ACQ to enter required transaction information 150 (FIG. 5), and manages the establishment of the private key 76, which is thereafter associated with the acquired certificate 60. As described above, the private key 76 may be submitted by the acquirer ACQ during the acquisition transaction 72, or may alternately be communicated to the acquirer ACQ from the certificate authority 12 during the acquisition transaction 72.

Alternate Embodiments for Payment Transfer. The certificate system 60 is easily adapted to provide alternate systems for payment transfer. For example, as described below, funds may be transferred directly from an acquirer payment agent 52 to a redeemer payment agent 56 upon the acquisition of a certificate 60, which is redeemed at a later time at a redemption location RL.

As well, funds may first be transferred directly from an acquirer payment agent 52 to a third party (*e.g.* such as to the certificate payment agent 58) upon the acquisition of a certificate 60, and from the certificate payment agent 58 to the redeemer payment agent 56 upon redemption.

In an alternate embodiment, an independent entity operates the certificate system 10, purchases virtual certificates 60 from one or more issuers 22, and then sells the purchased virtual certificates to acquirers, with funds transferring between the acquirer payment agents 52 to the certificate payment agent 58, either during the acquisition transaction, or during the redemption transaction 104.

Certificate Systems Having Payment Upon Acquisition. In one embodiment of the certificate system 10, payment funds are transferred from the acquirer payment agent 52 when a certificate 60 is acquired. While this payment

syst m may not b applicable for all mbodiments of the certificat system 10, payment of funds at th point of c rtificate acquisition 72 is often beneficial for issuers and redeemers, wherein inventory of goods, or reservations of services, are preferably held or reserved upon payment.

As well, for issuers, such as larger corporate clients, which are linked to a plurality of redemption locations RL (*e.g.* such as a chain of retail stores), inventory related to acquired certificates may be routed to a particular redemption location RL.

A certificate system 10 which offers payment upon certificate acquisition may be beneficial for "in-house" certificate systems 10, wherein the certificate authority 12 is a dedicated system for an issuer ISR, as seen in the certificate network 260b of Figure 16. However, for issuers and redeemers which may be small or unknown businesses, acquirer users ACQ may be hesitant to transfer funds from their respective acquirer payment agent 52 until the goods or services are deemed to be acceptable (*i.e.* at the point of redemption). For large or known issuers ISR, redemption locations RL, and for brand name products, payment upon acquisition may be satisfactory for acquirer users ACQ.

Certificate Systems Having Payment Upon Redemption Transaction. In a preferred embodiment of the certificate system 10, the certificate authority 12 receives an initial authorization to transfer funds from an acquirer payment agent 52, whereby the certificate authority establishes a "lock" on funds as a part of the certificate acquisition transaction 72. The funds are then transferred, from the acquirer payment agent 52 to the redeemer payment agent 56, when a certificate is redeemed 90,104 for actual goods or services, when the redemption transaction is authorized by the certificate authority 12 (*e.g.* such as by an authentication module 16).

For a certificate system 10 which serves a plurality of issuers ISR, payment upon redemption is often advantageous to acquirer users ACQ. For example, in a large independent certificate system 10, which accepts a plurality of issuers ISR, and allows acquirers ACQ to acquire certificates 60 for a selection of goods and services from the plurality of issuers ISR, it is important that only qualified and legitimate issuers be allowed to market certificates 60. As well, it is important that the issuers ISR clearly describe the products and services which are to be acquired through a redemption of an acquired certificate 60.

For a system in which payment of funds from an acquirer user ACQ is made upon the actual receipt of acceptable products or services, the acquirer ACQ (or alternate recipient RCP) is assured that redemption location RL, as well as the products or services to be received, are legitimate. It is therefore advantageous that issuers and redeemers clearly describe the goods or services which are represented by an acquired certificate 60.

As well, for a certificate system 10 in which payment of funds from an acquirer is made upon the actual receipt of acceptable products or services, the redemption transaction 104 is a true sales transaction, wherein the sale is independent of the certificate entity (except for the authorization to transfer funds). For example, funds are not transferred into or out of a certificate authority account 58, and an acquirer is able to accept or decline the transfer of funds at the time of the redemption transaction 104 (either by redeeming the certificate 60, or by declining a redemption). In such a certificate system, the certificate authority 12 need not accept responsibility for the quality of goods or services, since the redeemer receives funds from the acquirer payment agent 52 during the redemption transaction 104, and the acquirer receives the related goods or services from the redemption location RL during the redemption transaction 104.

Therefore, while an issuer ISR creates a virtual certificate 60 which is acquired through the certificate transaction network 10, the purchase transaction for the goods or services represented by the certificate occurs at the redemption location RL, typically through the merchant's point of sale terminal 40, with final redemption authorization of acquirer funds handled by the certificate authority 12.

In the preferred certificate system 10 wherein payment is not transferred until actual redemption of the certificate 60, buyers are inherently protected from misrepresented goods or services, or from illegitimate certificate issuers ISR. If a customer, such as an acquirer user, or a recipient of a certificate 60 (and accompanying private key 76), decides not to redeem the certificate, or upon visiting a redemption location RL, decides against the transaction for any reason, the customer may, at their discretion, decide against proceeding with the redemption transaction 104. Since the customer is not charged for the sale unless a redemption transaction 104 is actually made, the customer is inherently

protected, since th certificate system 10 minimizes misrepresentation of goods and services by issuers ISR.

For an acquirer ACQ who decides not to proceed with a redemption transaction 104, the acquirer ACQ may simply let the acquired certificate 60 "expire", or may actively return to the purchasing site, such as through the acquirer facilities 26, and actively cancel the certificate 60, while suspending the authorized lock on the acquirer's funds.

The enhanced level of protection for the buyer provided by the preferred certificate system 10 is advantageous for many redemption circumstances. While many business and personal travelers commonly purchase travel tickets (*e.g.* such as airline tickets, train tickets, accommodations, and car rentals) at the present time, funds are still transferred when the tickets are sent to or reserved for the acquirer ACQ or alternate recipient RCP. If travel plans are changed, or if flights are changed, buyers have little or no financial leverage. In contrast to conventional ticketing and reservations, if travel plans are changed, or if a flight is canceled, a customer in possession of an applicable certificate 60 can easily modify their travel plans, without being charged.

While authorization to charge against an acquirer's payment agent 52 (*e.g.* such as a credit card) is first established at the time the acquirer first acquires a certificate 60, funds are not typically transferred during the initial authorization. Instead, the initial authorization acts to validate an acquirer's payment agent 52, while performing a preliminary test for funds, which are to be typically charged later, during a second redemption transaction 104.

The second authorization against the acquirer's funds takes place when the certificate is redeemed. While the initial authorization typically confirms available credit for an acquirer, and typically establishes a hold on appropriate funds for the certificate 60, the fund hold may either be held in place indefinitely until redemption, or may expire before the redemption of the certificate. For a fund hold which expires before a certificate is redeemed, a redeemer may preferably still gain authorization to charge the acquirer's payment agent 52, during the redemption transaction 90 (such as by re-entering the credit information).

The preferred certificate system 10 therefore provides a mutually safe and fair means for commerce between an acquirer and an issuer, since, the acquirers ACQ are properly authorized (both during the initial acquisition of the certificate and during the redemption transaction 104), while the holder of the certificate 60 (*i.e.* the acquirer or an authorized recipient of an acquired certificate) is also able to accept or decline the redemption transaction 90 (*e.g.* such as upon visiting the redemption location, if the goods or services are not satisfactory).

In this preferred embodiment of the certificate system, funds are never transferred to the hosting certificate system 10, but are only transferred, upon a redemption transaction 104, from the acquirer payment agent 52, either to the issuer payment agent 54, or to the redeemer payment agent 56. In this mode of operation, a second authorization is required at the time the certificate is redeemed, to authorize transfer of funds, and to initiate the actual transfer of funds.

Financial institutions which offer credit card systems typically charge merchant businesses different discount rates (*e.g.* typically a percentage of each sale), based upon the type of sales transactions. Many financial institutions charge different rates for credit card "present" transactions, credit card "not present" transactions, and internet transactions, with the greatest rates typically charged to internet transactions (typically since fraudulent use of credit cards is currently more prevalent on the internet).

However, within the certificate system 10, for embodiments where funds are initially locked during the acquisition, and where a second authorization takes place upon redemption of an acquired certificate, funds are transferred at the redemption level. For an acquirer user ACQ who has a card present for redemption authorization, there is a reasonable level of security for the merchant that the card is valid. Even for an acquirer ACQ or recipient RCP who is in possession of the certificate 60 and the private key 76, the redemption transaction is significantly more secure than a remote internet transaction. Therefore, a merchant is more likely to pay less to the credit card issuing agency.

System Structures. The certificate system 10 may operate across a wide variety of networks 192, and may be easily adapted to promote various commerce models. Figure 15 shows one network embodiment 260a of a certificate system 10 implemented across a network 192, having a plurality of

issuer t rminals 22a-22p, ach having issuer facilities 24a-24p, and network connection 23a-23p; a remote certificate authority 12, including a certificat module 14, an authentication module 16, a database 18, and an authority terminal 58; and a plurality of redeemer facilities 38a-38q (typically located at one or more redemption locations RL). A plurality of acquirer terminals 26a-26n, each having acquirer facilities 28a-28n, and network connections 27a-27n, are connected to network 192, such that a plurality of acquirer users may browse and acquire certificates 60 which are created by a plurality of issuer users at issuer terminals 22a-22p.

Figure 16 shows an embodiment of an alternate network embodiment 260b of a certificate system 10 implemented across a network 192 having a single issuer terminal 22, with an issuer facility 24, having a network connection 23; and a related dedicated certificate authority 12, including a certificate module 14, an authentication module 16, a database 18, and an authority terminal 58. For a large issuer ISR, such as a conglomerate which provides a large selection of products or services at a plurality of redeemer facilities 38a-38q, located at one or more redemption locations RL, a dedicated certificate authority system 12,14,16,18,58 may preferably be used to manage a large virtual inventory of 228 certificates 60 on an issuer network site 242. A plurality of acquirer terminals 26a-26n, each having acquirer facilities 28a-28n and network connections 27a-27n, are connected to network 192, such that a plurality of acquirer users ACQ may browse and acquire certificates 60 within the virtual inventory 228 of the merchant site 242.

System Applications and Alternative Embodiments. The certificate system 10 can be used for a large variety of commerce applications, wherein products and services are located on-line, but are picked up at a store RL. For example, an acquirer user ACQ may locate a large gift item on-line (*e.g.* such as a television set), which can be picked up at a location RL near a recipient RCP. The acquirer user ACQ may simply search for and locate the desired gift item at a location RL near the recipient RCP, proceed with an acquisition transaction 72, transfer the acquired certificate 60 (or just the certificate information 74) to the recipient RCP (or directly to the redemption location RL), and communicate the private key to the recipient RCP. The recipient RCP may then perform the redemption transaction 90, and receive the gift item.

In a similar mbodiment, an acquirer user ACQ may desire to send a gift certificate with a selected money denomination 64 to a recipient RCP. With th certificate information 74 and the private key 76, the recipient RCP can either visit the redemption location RL directly, or may alternately browse on-line through an aggregate site 234 or a merchant site 242, to locate desired goods or services, before picking the desired goods up at the redemption location RL.

The certificate system 10 can also be used for travel and accommodations, and for various ticketing applications. As well, the certificate system 10 may be used as a secure currency, in the form of "traveler's" certificates, which are acquired online, but are spent or cashed at one or more locations RL. As well, the certificate system may be used to prepay for services, such as for medical or dental services, or even home repair.

The certificate system 10 may be alternately used for business vouchers systems, in which personnel, such as employees, are sent to pick up and deliver goods and services, using single-use certificates 60 to provide for the secure transfer of various forms of inventory.

As described above, the certificate system 10 does not require that monetary funds are transferred, or that the system be used exclusively for purchasing products or services. For example, the certificate system 10 may be used to distribute discount coupons for one or more issuers ISR, which are typically redeemable as a discount for an acquired product or service. While virtual coupons are similar to virtual certificates 60, there is typically no monetary value associated with a virtual coupon, such that there may be no private key verification required during a redemption transaction 90. An acquirer user ACQ simply accesses a desired virtual coupon (*e.g.* such as for a related search for products or businesses within their regional area), and prints a desired coupon on an acquirer printer 30. The acquirer user ACQ may then visit a related redemption location RL (*i.e.* the selected store), which honors and redeems the coupon (typically as a discount for a product or service specified on the virtual coupon).

A merchant issuer may preferably combine the use of virtual certificates 60 with that of virtual coupons, such as through a virtual site, wherein an acquirer user may receive a discount that is related to the acquisition of one or more certificates 60.

For exampl , to promot the redemption location RL, an issuer user may provid an acquir r user with a virtual discount coupon, as a bonus for prior certificate purchases.

System Advantages. Retailers, such as small merchants or service providers, may easily establish means for selling their goods and services online, without the requirement of establishing an extensive online presence. Issuers may simply register their business with the certificate authority 12, and then may create virtual certificates 60 for one or more of their products and services. Virtual certificates 60 can be offered for acquisition at one or more network sites, such as an aggregated site 234 for a large variety of products and services within a selected region, or a more specialized site 234 that is related to specific types of products or services within their area.

As well, even without a web site, an issuer/merchant can input other store information 251a,251b (such as business location information, logos, product descriptions), which is then displayed on a web page 248,252 appropriate to a virtual certificate 60, along with credit cards 52 which are acceptable to the issuer/merchant. When an acquirer ACQ navigates to a description 251 of a virtual certificate within a virtual site 248, such as by limiting a search to a specific product category within a specified zip code region, the issuer/merchant information 251 is preferably displayed, in conjunction with the virtual certificate 60, thereby creating a network presence for the issuer/merchant. As well, if an acquirer ACQ selects the certificate 60 (*i.e.* decides to acquire the certificate), the acquirer facility 28 typically displays an acquisition invoice module 252 that is specific to an issuer/merchant for the selected certificate 60, wherein selectable payment agent information (*i.e.* accepted credit cards) are limited to cards which the issuer accepts at the redemption location RL.

Through the certificate system 10, acquirers are able to find goods and services that they might not have been able to find otherwise. As well, acquirers are able to secure a price for a transaction at the time they acquire a certificate 60. While the certificate authority 12 creates a virtual inventory 228 of virtual certificates 60 which may be used to browse and shop through aggregate sites 234 or dedicated sites 242, there is no inventory of paper-based certificates or coupons.

Although th certificate syst m 10 and its m thods of use ar described h rein in connection with retail certificates off red through web sites, the apparatus and techniques can be implemented for other certificate, coupon, voucher, or token systems, and over different types of networks, or any combination thereof, as desired.

Accordingly, although the invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow.

CLAIMS

What is claimed is:

1. A certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate including said redemption denomination and said first public key identifier, said creation of said issued certificate including a private key assigned at time of said acquisition of said virtual certificate, wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of a redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal of said redemption denomination, said first public key identifier, and said private key, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

2. The certificate system of Claim 1, wherein said defined virtual certificate includes a second public key identifier defined by said issuer user, wherein said second public key identifier is stored at said certificate authority, and wherein said authorization module requires a submittal of said second public key identifier, and a matching comparison to said second public key identifier stored at said certificate authority.

3. The certificate system of Claim 1, wherein said a certificate issuance module requires the submittal of a payment agent by said acquirer user.

4. The certificate system of Claim 3, wherein said required submittal of said payment agent for said acquirer user includes an authorization to transfer funds from said payment agent for said acquirer upon creation of said issued certificate.

5. The certificate system of Claim 3, wherein said required submittal of said payment agent for said acquirer user includes an authorization to transfer funds from said payment agent for said acquirer upon redemption of said issued certificate.

6. The certificate system of Claim 1, wherein said certificate issuance module includes means to deliver said redemption denomination, said first public key identifier, and said entered private key to said acquirer user.

7. The certificate system of Claim 6, wherein said means to deliver said redemption denomination, said first public key identifier, and said entered private key to said acquirer user comprises a printed form of said issued certificate.

8. The certificate system of Claim 6, wherein said means to deliver said redemption denomination, said first public key identifier, and said entered private key to said acquirer user comprises an electronic form of said issued certificate.

9. The certificate system of Claim 1, wherein said holder of said issued certificate is said acquirer user.

10. The certificate system of Claim 1, wherein said holder of said issued certificate is an alternate recipient who submits said private key.

11. The certificate system of Claim 1, wherein said assigned private key is entered by said acquirer user during said selectable acquisition of said virtual certificate.

12. The certificate system of Claim 11, wherein said entered, assigned private key is unique to a single acquired issued certificate.

13. The certificate system of Claim 11, wherein said entered, assigned private key is a private purchase key unique to said acquirer user.

14. The certificate system of Claim 11, wherein said entered, assigned private key is a private acquirer facility access key unique to said acquirer user.

15. The certificate system of Claim 1, wherein said assigned private key is established by said certificate authority during said selectable acquisition of said virtual certificate.

16. A process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate including said redemption denomination and said first public key identifier, said creation of said issued certificate including an establishment a private key, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing a redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal of said redemption denomination, said first public key identifier, and said private key, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

17. The process of Claim 16, wherein said step of defining said virtual certificate,

wherein said defined virtual certificate includes a second public key identifier defined by said issuer user, wherein said step of creating said issued certificate includes the storage of said second public key identifier at said certificate authority, and wherein said step of authorizing said redemption of said issued certificate includes a submittal of said second public key identifier, and a matching comparison to said second public key identifier stored at said certificate authority.

18. The proc ss of Claim 16, wherein said step of creation of said issued certificate includes th submittal of a payment agent by said acquirer user.

19. The process of Claim 18, wherein said submittal of said payment agent for said acquirer user includes an authorization to transfer funds from said payment agent for said acquirer during said step of creation of said issued certificate.

20. The process of Claim 18, wherein said submittal of said payment agent for said acquirer user includes an authorization to transfer funds from said payment agent for said acquirer during said step of redemption of said issued certificate.

21. The process of Claim 16, wherein said step of creation of said issued certificate includes a delivery of said redemption denomination, said first public key identifier, and said entered private key to said acquirer user.

22. The process of Claim 21, wherein said delivered redemption denomination, said first public key identifier, and said entered private key to said acquirer user are included in a printed form of said issued certificate.

23. The process of Claim 21, wherein said delivered redemption denomination, said first public key identifier, and said entered private key to said acquirer user are included in an electronic form of said issued certificate.

24. The process of Claim 16, wherein within said authorizing step, said holder of said issued certificate is said acquirer user.

25. The process of Claim 16, wherein within said authorizing step, said holder of said issued certificate is an alternate recipient which submits said private key.

26. The process of Claim 16, wherein said established private key is entered by said acquirer user.

27. Th process of Claim 26, wherein said entered established privat k y is unique to a single acquired issued certificate.

28. The process of Claim 26, wherein said entered established private key is a private purchase key that is unique to said acquirer user.

29. The process of Claim 26, wherein said entered established private key is a private acquirer facility access key that is unique to said acquirer user.

30. The process of Claim 16, wherein said established private key is established by said certificate authority and communicated to said acquirer.

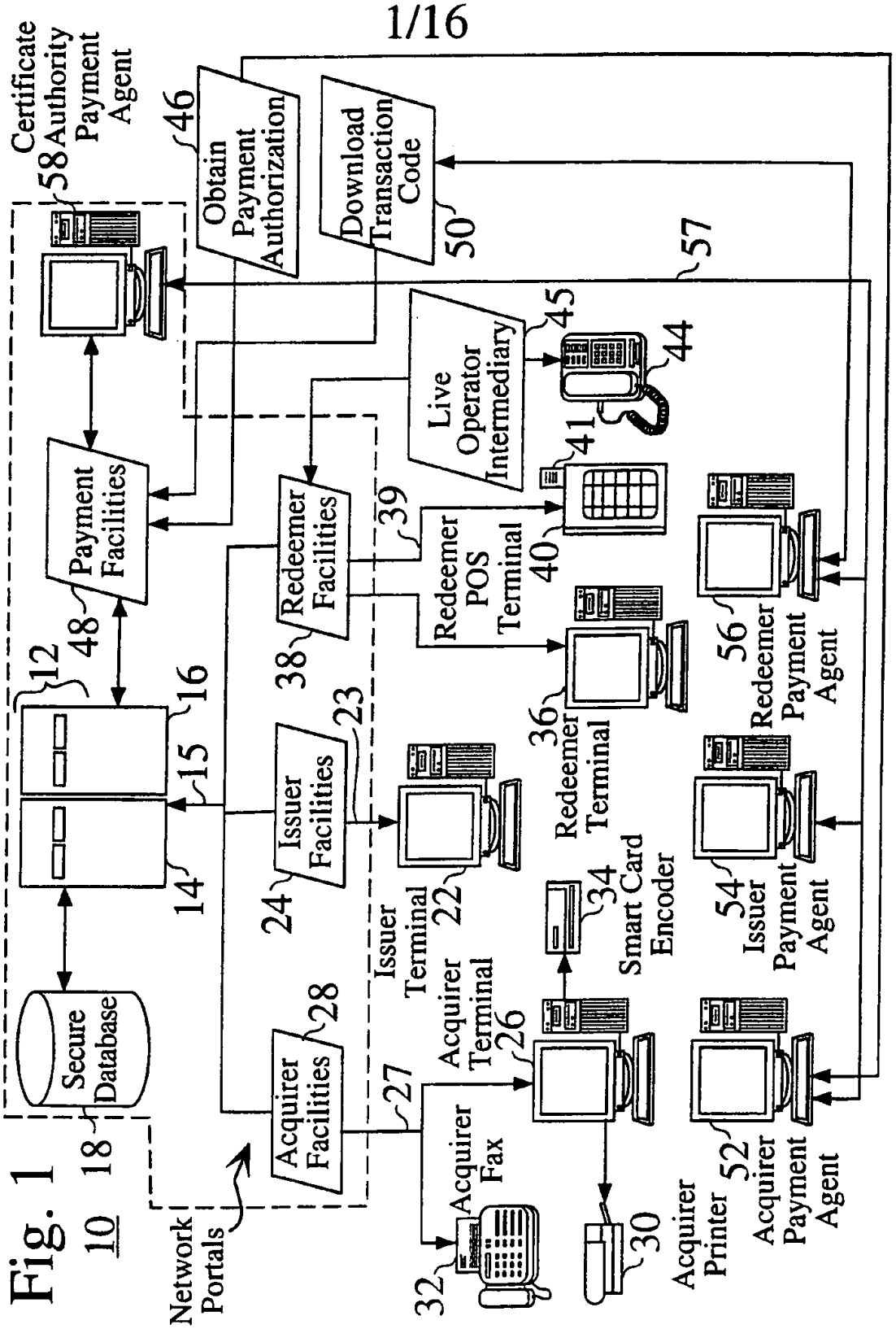

Certificate Authority Payment Agent
58
Obtain Payment Authorization
46
Download Transaction Code
50
57
Live Operator Intermediary
45
44
41
Payment Facilities
48
12
16
15
14
Redeemer Facilities
38
39
Redeemer POS Terminal
40
Redeemer Terminal
36
56
Redeemer Payment Agent
Issuer Facilities
23
24
Issuer Terminal
22
Smart Card Encoder
34
54
Issuer Payment Agent
Secure Database
18
Acquirer Facilities
28
27
Acquirer Terminal
26
Acquirer Fax
32
30
Acquirer Printer
52
Acquirer Payment Agent
Network Portals
10

Fig. 1

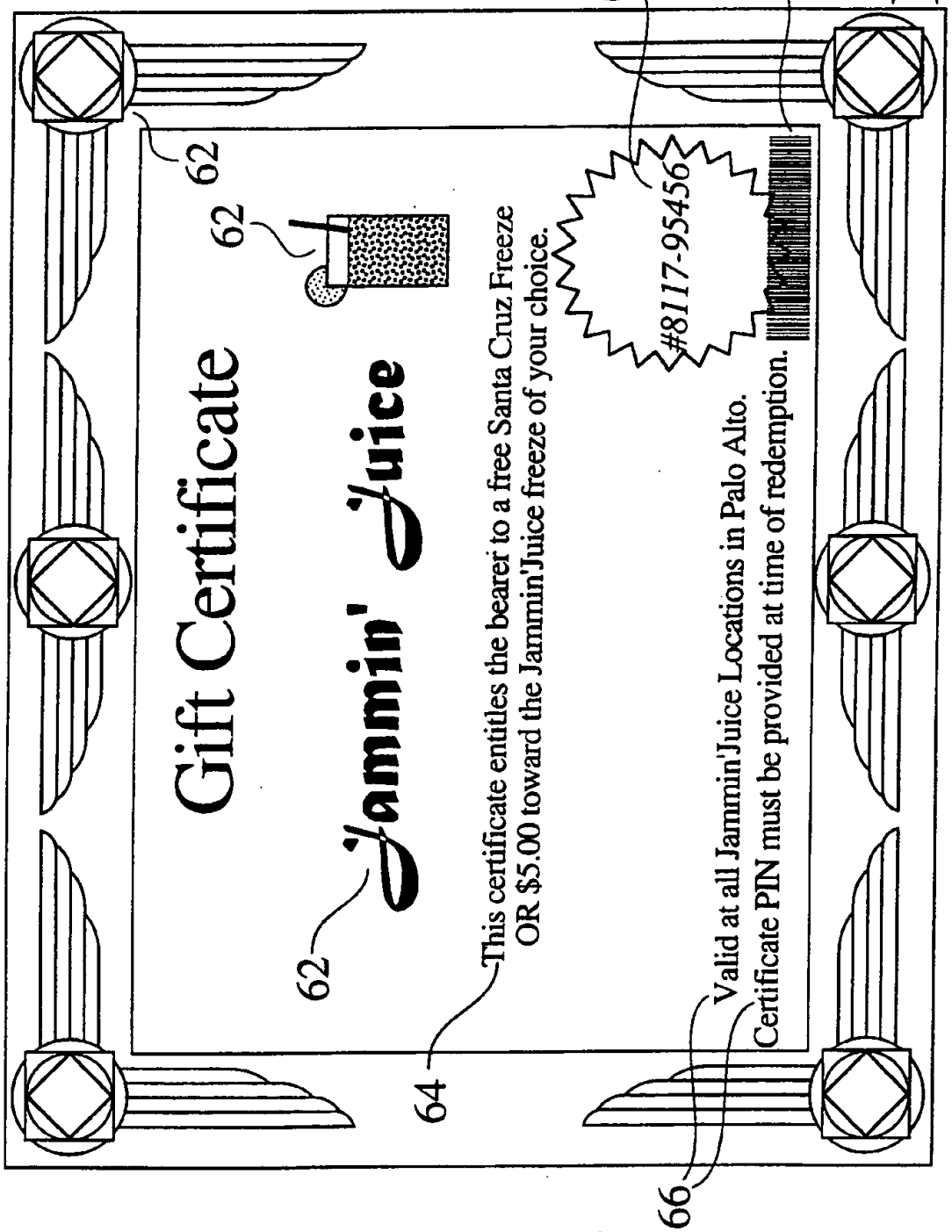

60
62
62
62
Gift Certificate
Jammin' Juice
This certificate entitles the bearer to a free Santa Cruz Freeze
OR $5.00 toward the Jammin'Juice freeze of your choice.
64
#8117-95456
68
70
Valid at all Jammin'Juice Locations in Palo Alto.
Certificate PIN must be provided at time of redemption.
66

Fig. 2

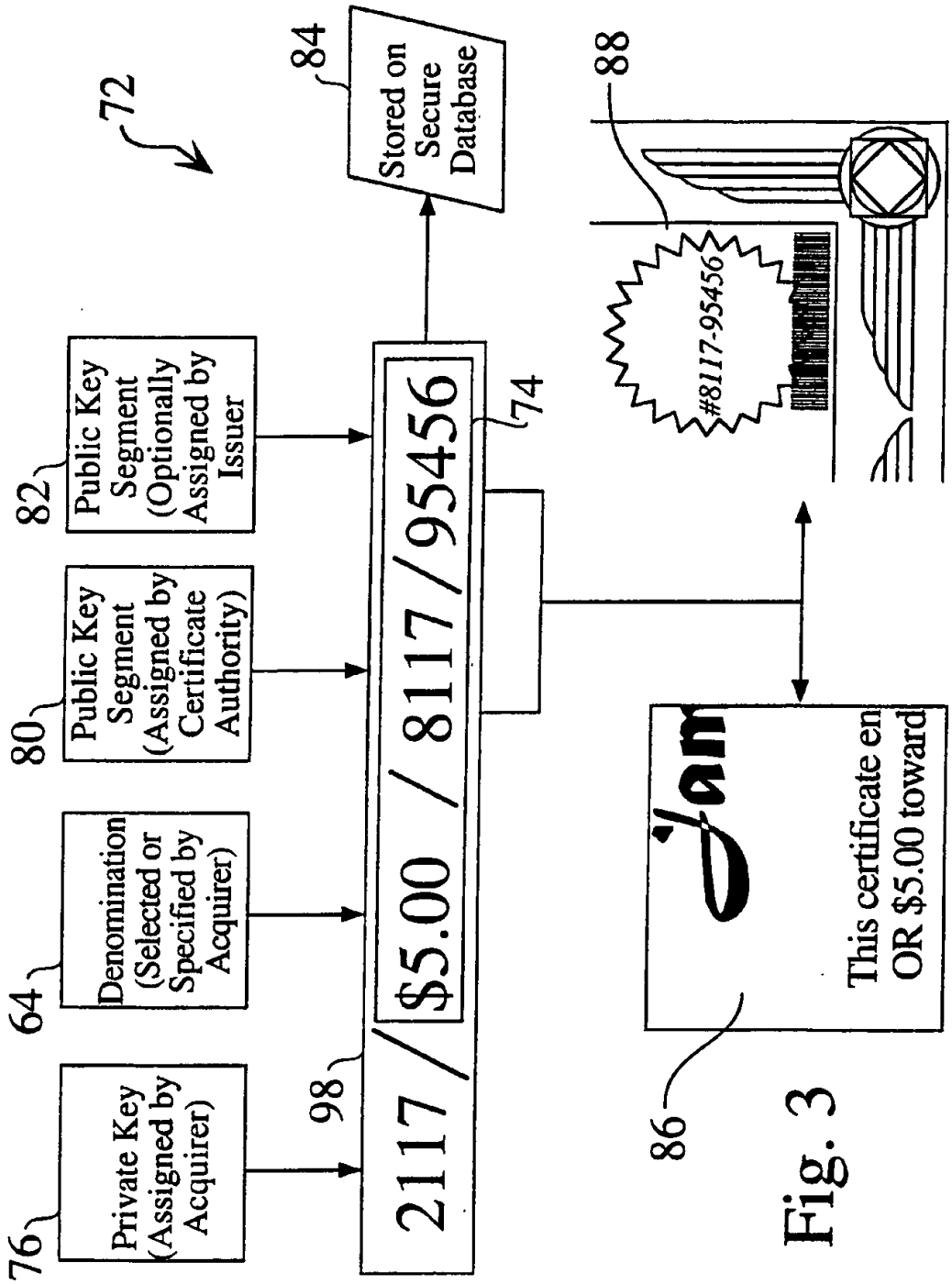

72
84
Stored on Secure Database
88
#8117-95456
82
Public Key Segment (Optionally Assigned by Issuer
80
Public Key Segment (Assigned by Certificate Authority)
64
Denomination (Selected or Specified by Acquirer)
76
Private Key (Assigned by Acquirer)
98
2117 / $5.00 / 8117 / 95456
74
86
This certificate en
OR $5.00 toward

Fig. 3

Fig. 4

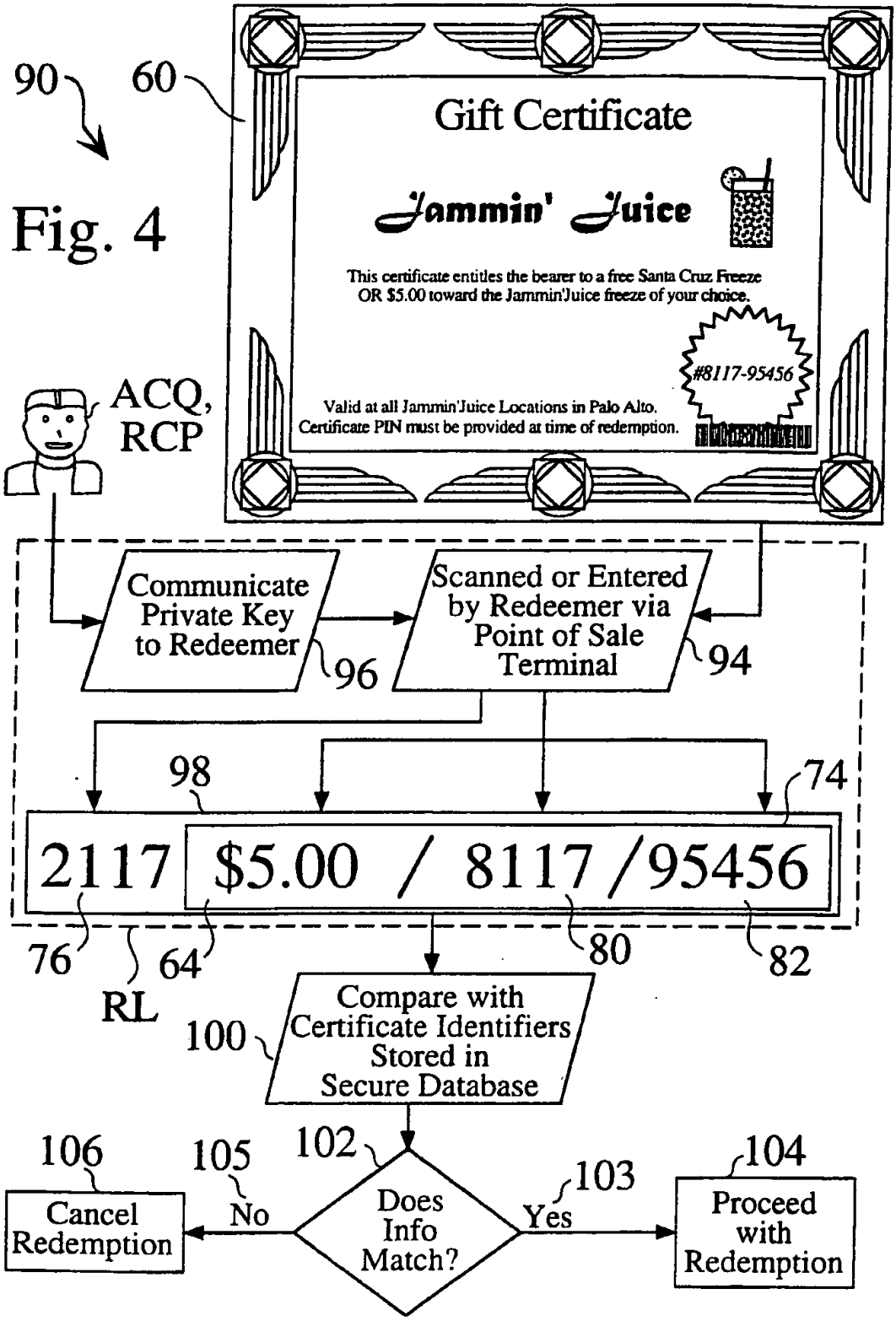

90
60
Gift Certificate
Jammin' Juice
This certificate entitles the bearer to a free Santa Cruz Freeze
OR $5.00 toward the Jammin'Juice freeze of your choice.
#8117-95456
Valid at all Jammin'Juice Locations in Palo Alto.
Certificate PIN must be provided at time of redemption.
ACQ, RCP
Communicate Private Key to Redeemer
96
Scanned or Entered by Redeemer via Point of Sale Terminal
94
98
74
2117
$5.00 / 8117 /95456
76
64
80
82
RL
100
Compare with Certificate Identifiers Stored in Secure Database
102
106
105
103
104
Cancel Redemption
No
Does Info Match?
Yes
Proceed with Redemption

Fig. 5

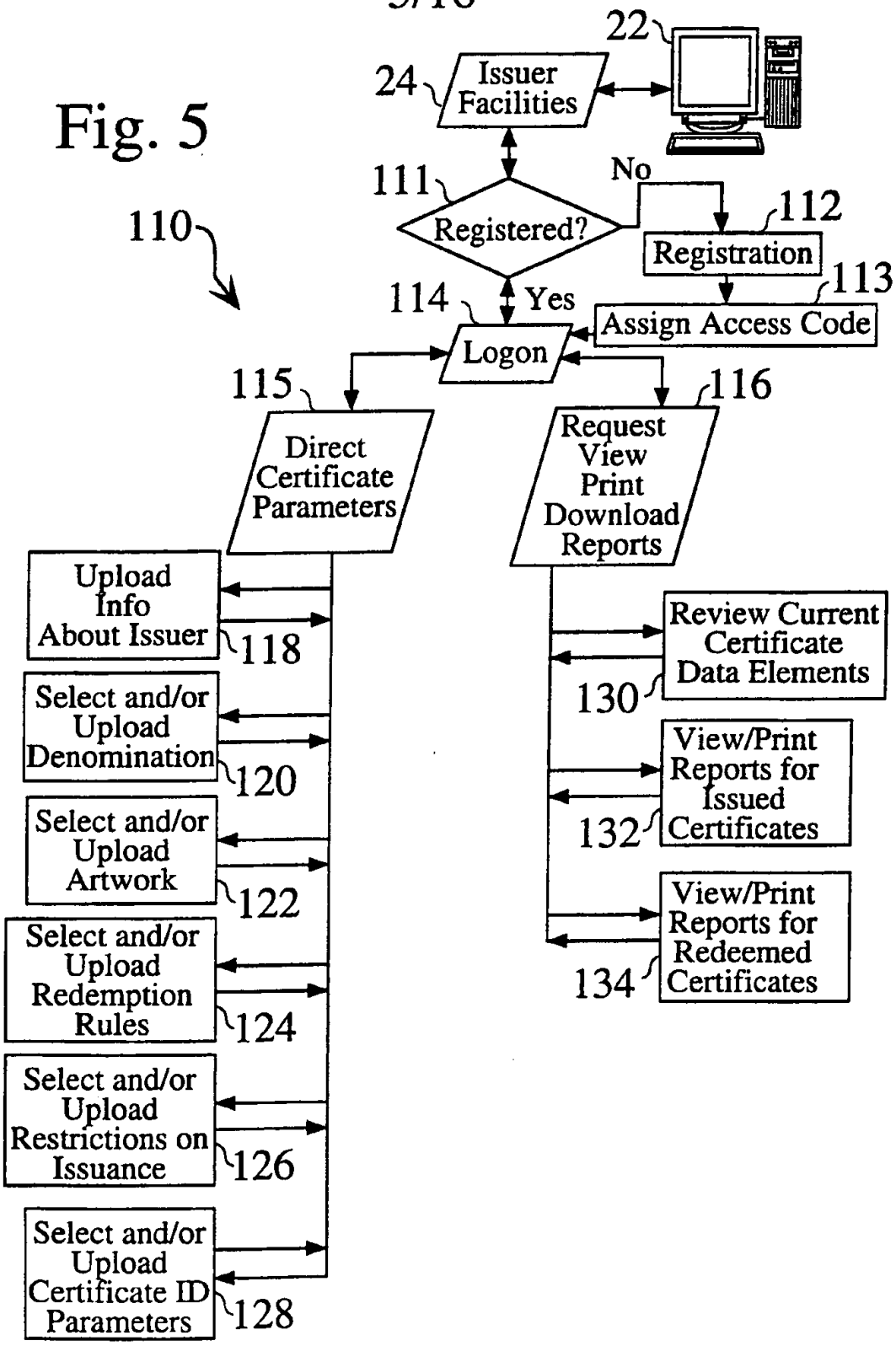

22
24
Issuer Facilities
110
111
Registered?
No
112
Registration
113
Assign Access Code
114
Yes
Logon
115
Direct Certificate Parameters
116
Request View Print Download Reports
Upload Info About Issuer
118
Select and/or Upload Denomination
120
Select and/or Upload Artwork
122
Select and/or Upload Redemption Rules
124
Select and/or Upload Restrictions on Issuance
126
Select and/or Upload Certificate ID Parameters
128
Review Current Certificate Data Elements
130
View/Print Reports for Issued Certificates
132
View/Print Reports for Redeemed Certificates
134

Fig. 6

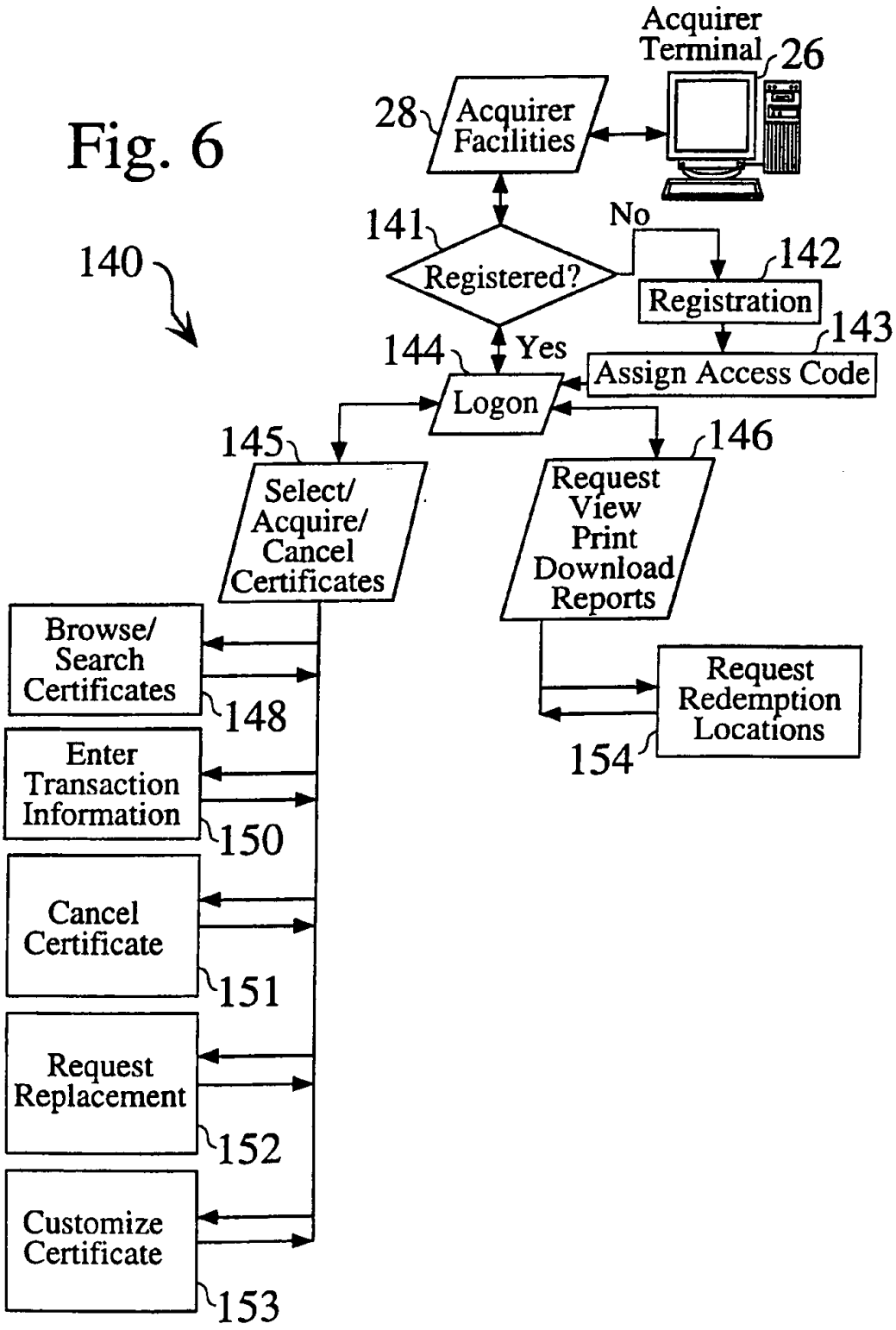
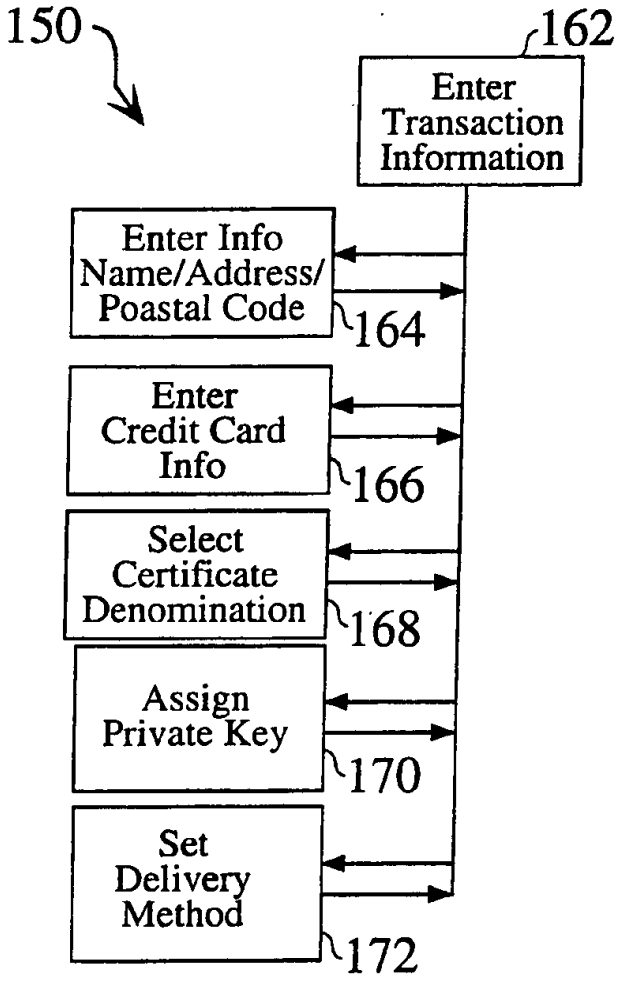

Acquirer Terminal
26
28
Acquirer Facilities
140
141
Registered?
No
142
Registration
143
Assign Access Code
144
Yes
Logon
145
Select/ Acquire/ Cancel Certificates
146
Request View Print Download Reports
Browse/ Search Certificates
148
Enter Transaction Information
150
Cancel Certificate
151
Request Replacement
152
Customize Certificate
153
Request Redemption Locations
154

Fig. 7


150
162
Enter Transaction Information
Enter Info Name/Address/ Poastal Code
164
Enter Credit Card Info
166
Select Certificate Denomination
168
Assign Private Key
170
Set Delivery Method
172

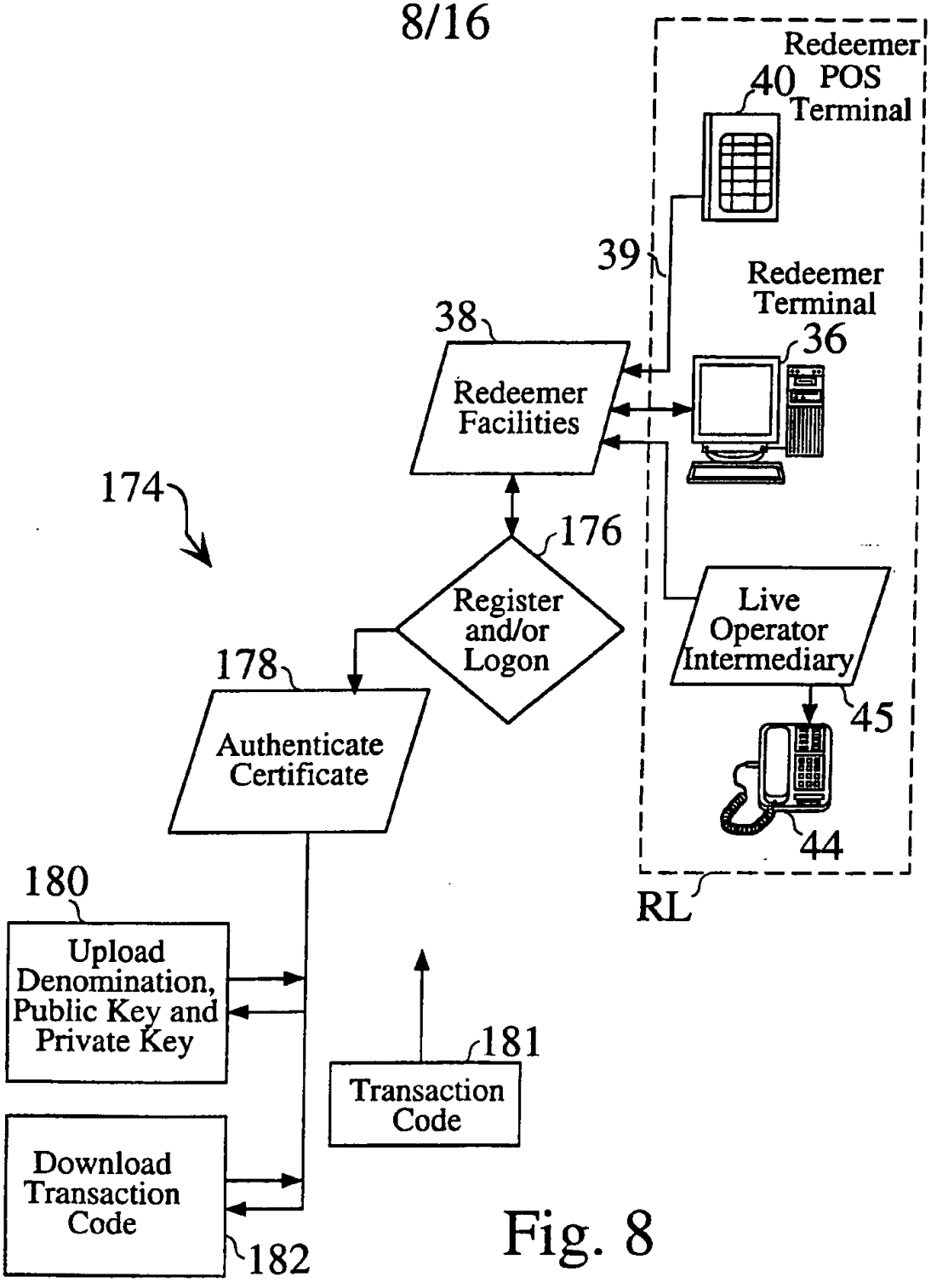

Redeemer
40 POS
Terminal
39
Redeemer
Terminal
36
38
Redeemer
Facilities
174
176
Register
and/or
Logon
Live
Operator
Intermediary
45
178
Authenticate
Certificate
44
RL
180
Upload
Denomination,
Public Key and
Private Key
181
Transaction
Code
Download
Transaction
Code
182

Fig. 8

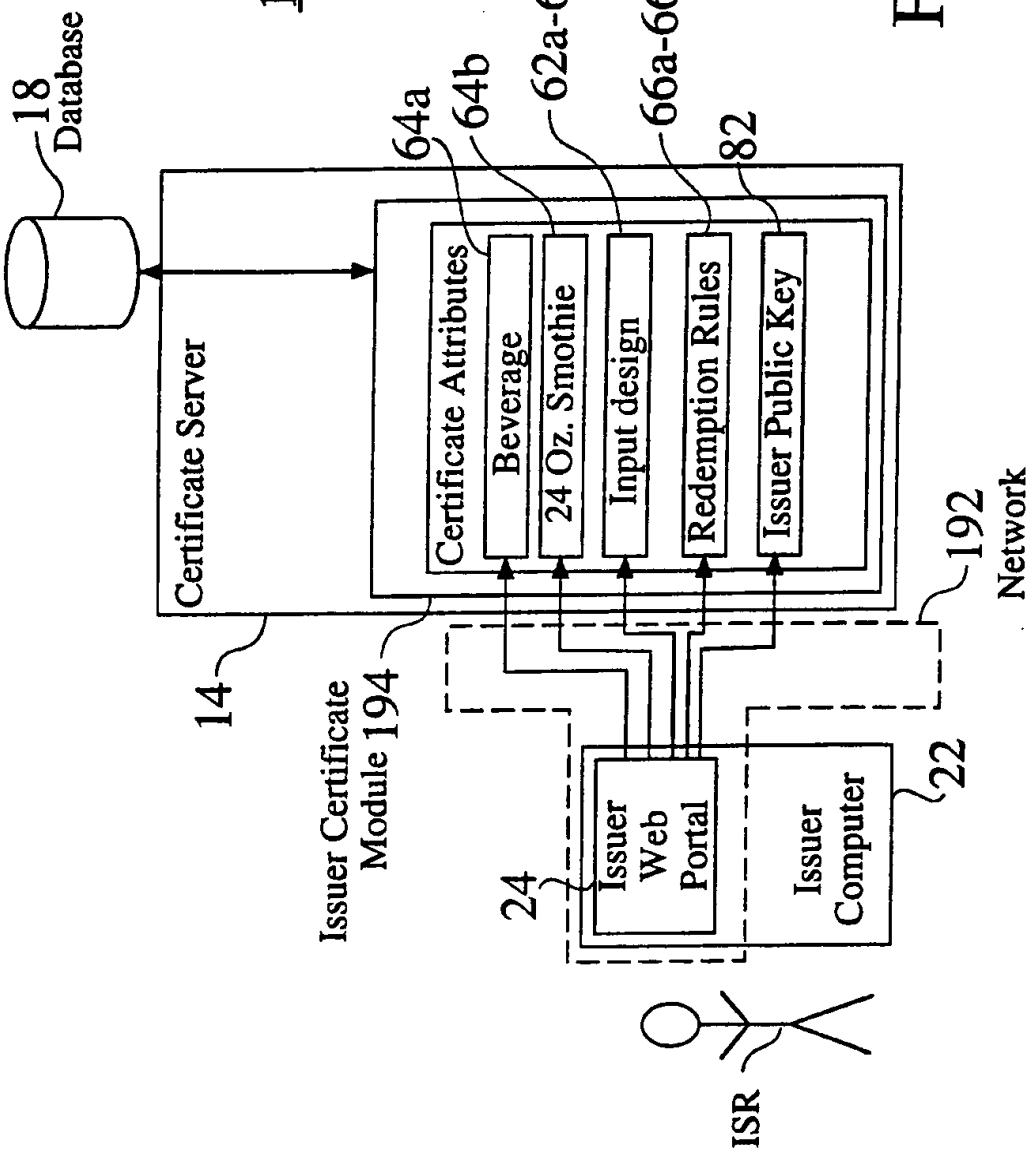

190
18
Database
64a
64b
62a-62n
66a-66n
82
Certificate Server
Certificate Attributes
Beverage
24 Oz. Smothie
Input design
Redemption Rules
Issuer Public Key
192
Network
14
Issuer Certificate
Module 194
24
Issuer
Web
Portal
Issuer
Computer
22
ISR

Fig. 9

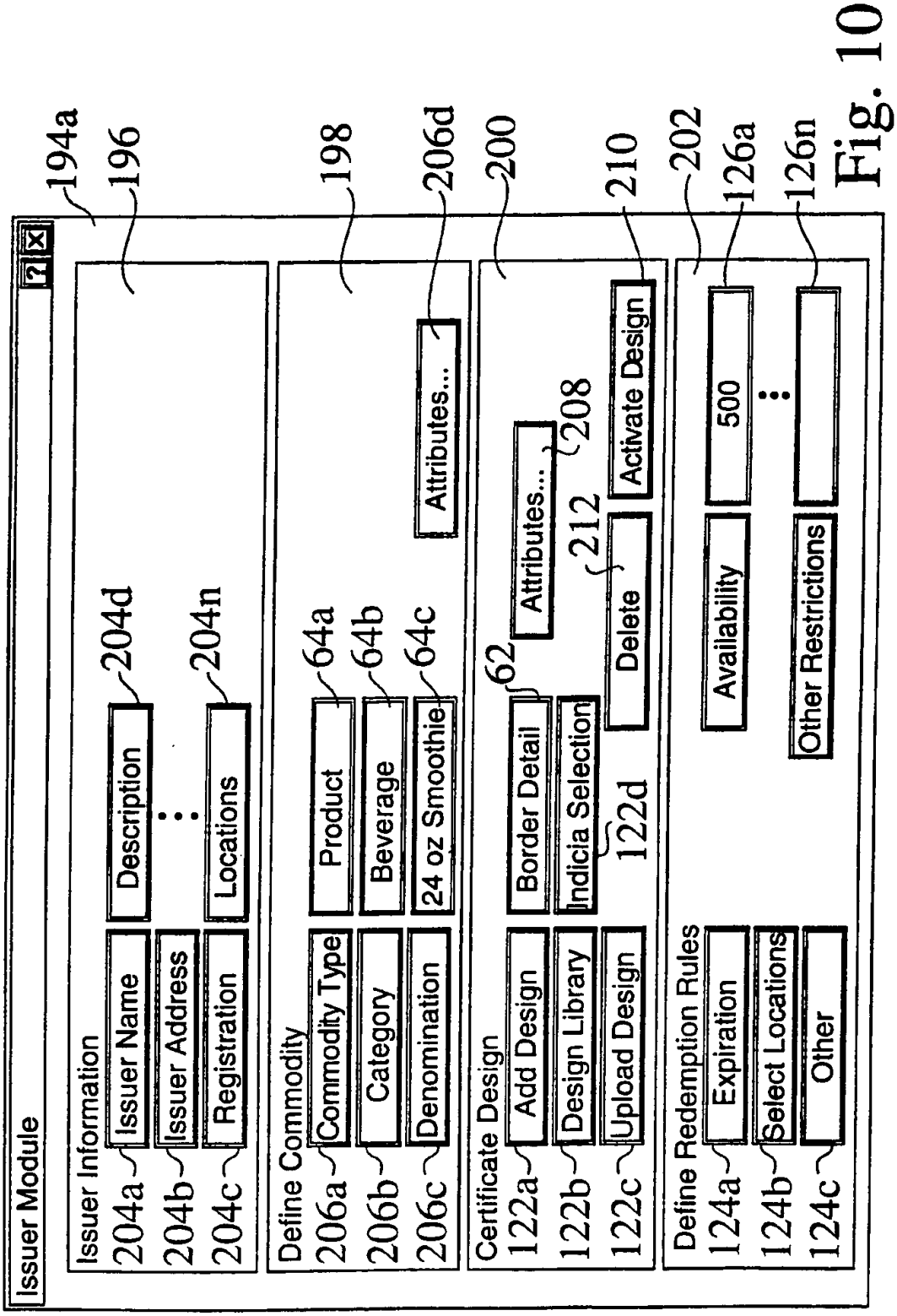

Issuer Module
194a
196
198
206d
200
210
202
126a
126n
Issuer Information
204a
204b
204c
Issuer Name
Issuer Address
Registration
Description
Locations
204d
204n
Define Commodity
206a
206b
206c
Commodity Type
Category
Denomination
Product
Beverage
24 oz Smoothie
64a
64b
64c
Attributes...
Certificate Design
122a
122b
122c
Add Design
Design Library
Upload Design
Border Detail
Indicia Selection
62
Attributes...
208
212
Delete
122d
Activate Design
Define Redemption Rules
124a
124b
124c
Expiration
Select Locations
Other
Availability
500
Other Restrictions

Fig. 10

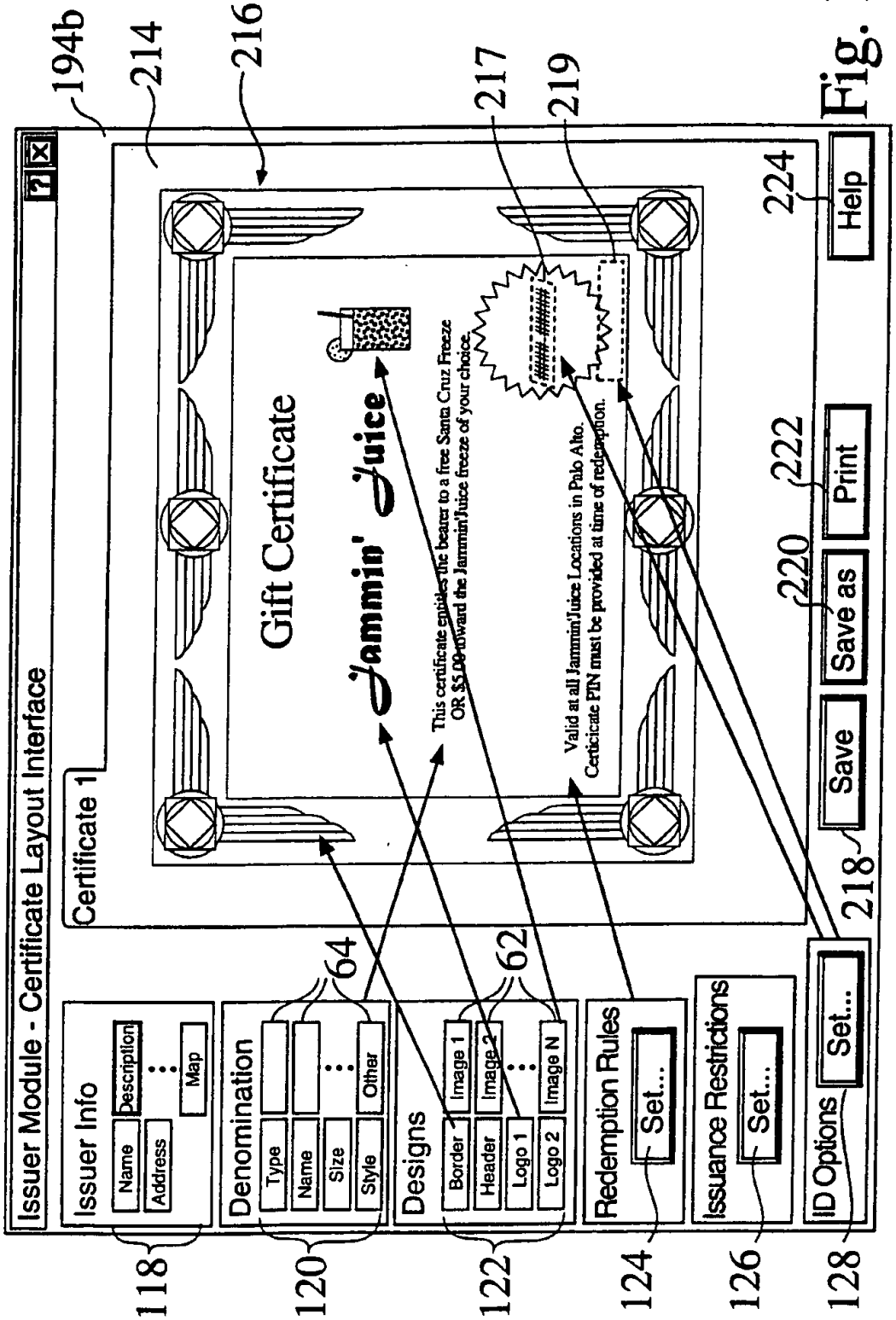

Issuer Module - Certificate Layout Interface
194b
214
216
217
219
224
Help
Gift Certificate
Jammin' Juice
This certificate entitles the bearer to a free Santa Cruz Freeze OR $5.00 toward the JamminJuice freeze of your choice.
######
Valid at all JamminJuice Locations in Palo Alto.
Certificate PIN must be provided at time of redemption.
Certificate 1
222
Print
220
Save as
Save
218
Issuer Info
Name
Address
Description
Map
Denomination
Type
Name
Size
Style
Other
64
Designs
Border
Header
Logo 1
Logo 2
Image 1
Image 2
Image N
62
Redemption Rules
Set...
Issuance Restrictions
Set...
ID Options
Set...
118
120
122
124
126
128

Fig. 11

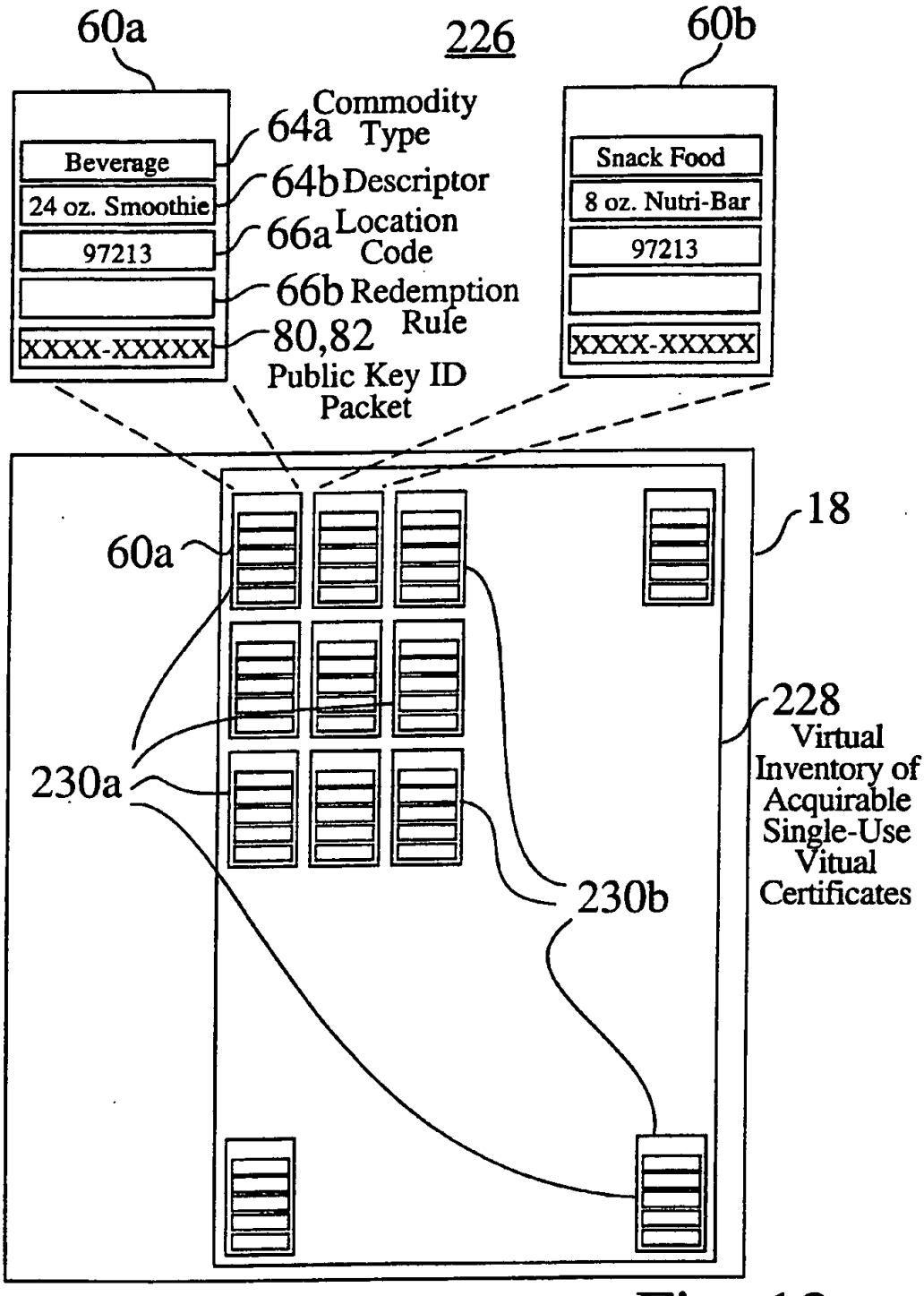

60a
226
60b
Commodity Type
64a
Beverage
64b Descriptor
24 oz. Smoothie
66a Location Code
97213
66b Redemption Rule
XXXX-XXXXX
80,82 Public Key ID Packet
Snack Food
8 oz. Nutri-Bar
97213
XXXX-XXXXX
18
60a
228 Virtual Inventory of Acquirable Single-Use Vitual Certificates
230a
230b

Fig. 12

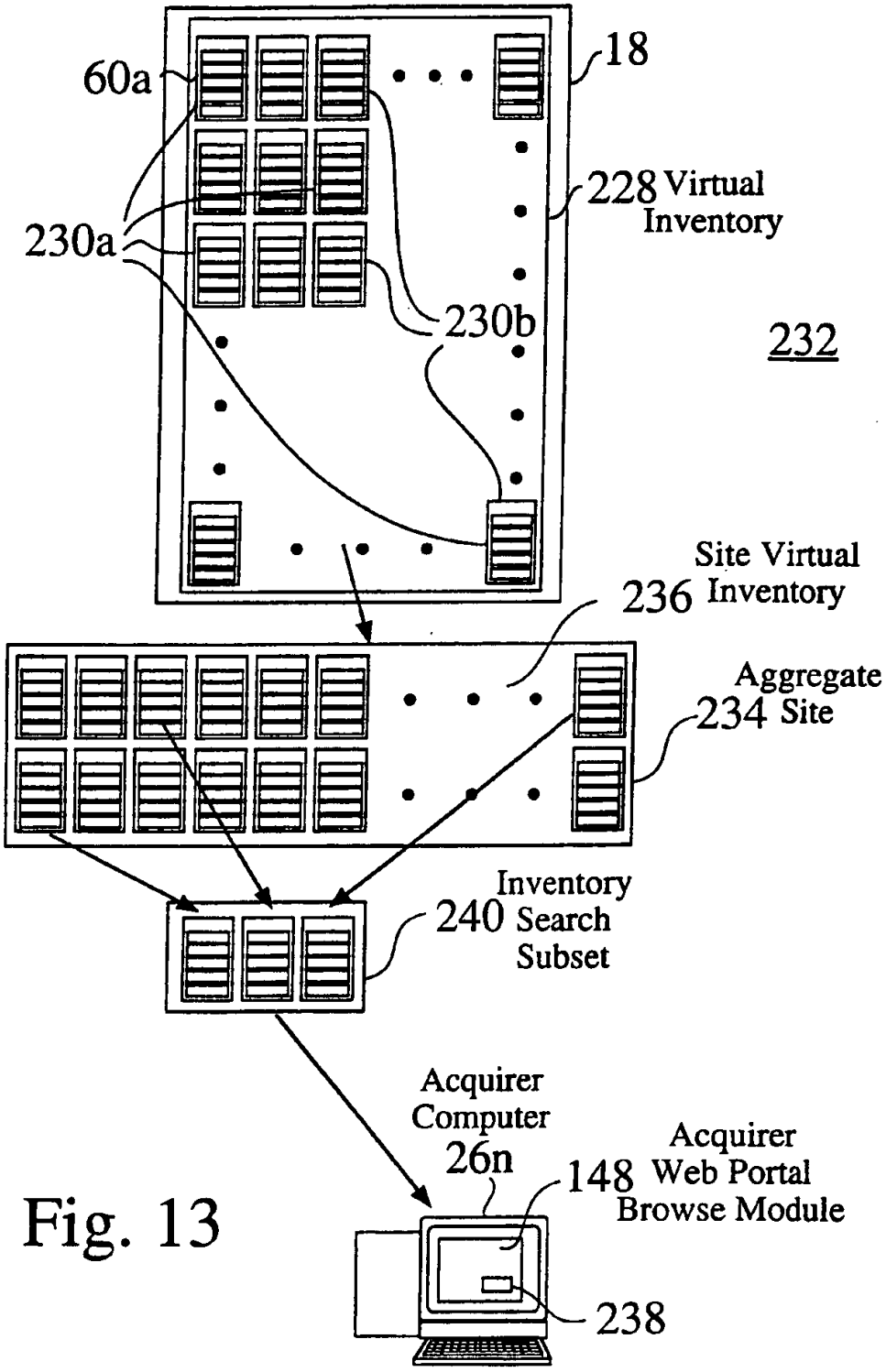

60a
18
228 Virtual Inventory
230a
230b
232
Site Virtual Inventory
236
Aggregate Site
234
Inventory Search Subset
240
Acquirer Computer
26n
148 Acquirer Web Portal Browse Module
238

Fig. 13

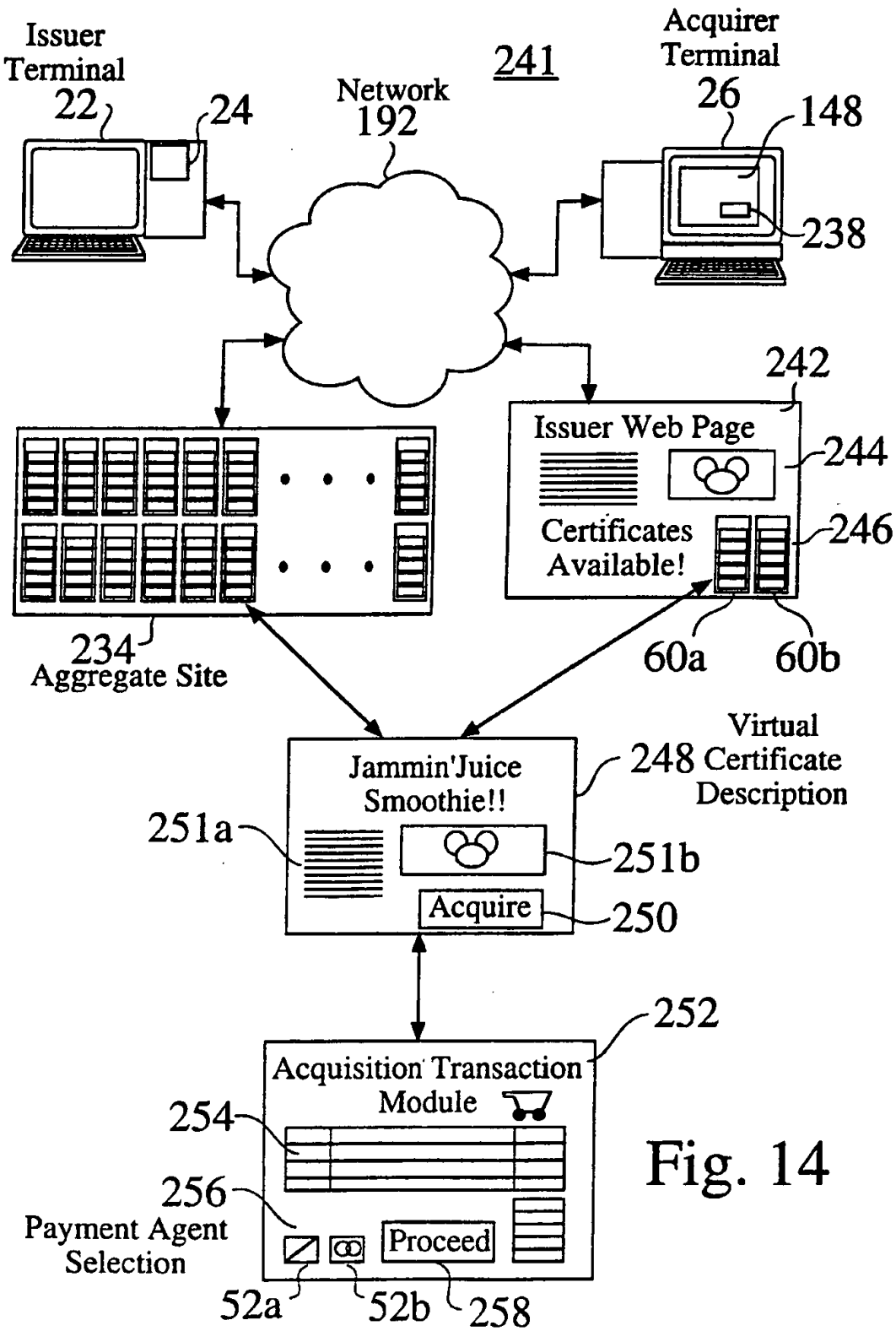

Issuer Terminal
22
24
241
Network
192
Acquirer Terminal
26
148
238
242
Issuer Web Page
244
Certificates Available!
246
234
Aggregate Site
60a
60b
Virtual Certificate Description
248
Jammin'Juice Smoothie!!
251a
251b
Acquire
250
252
Acquisition Transaction Module
254
256
Payment Agent Selection
Proceed
52a
52b
258

Fig. 14

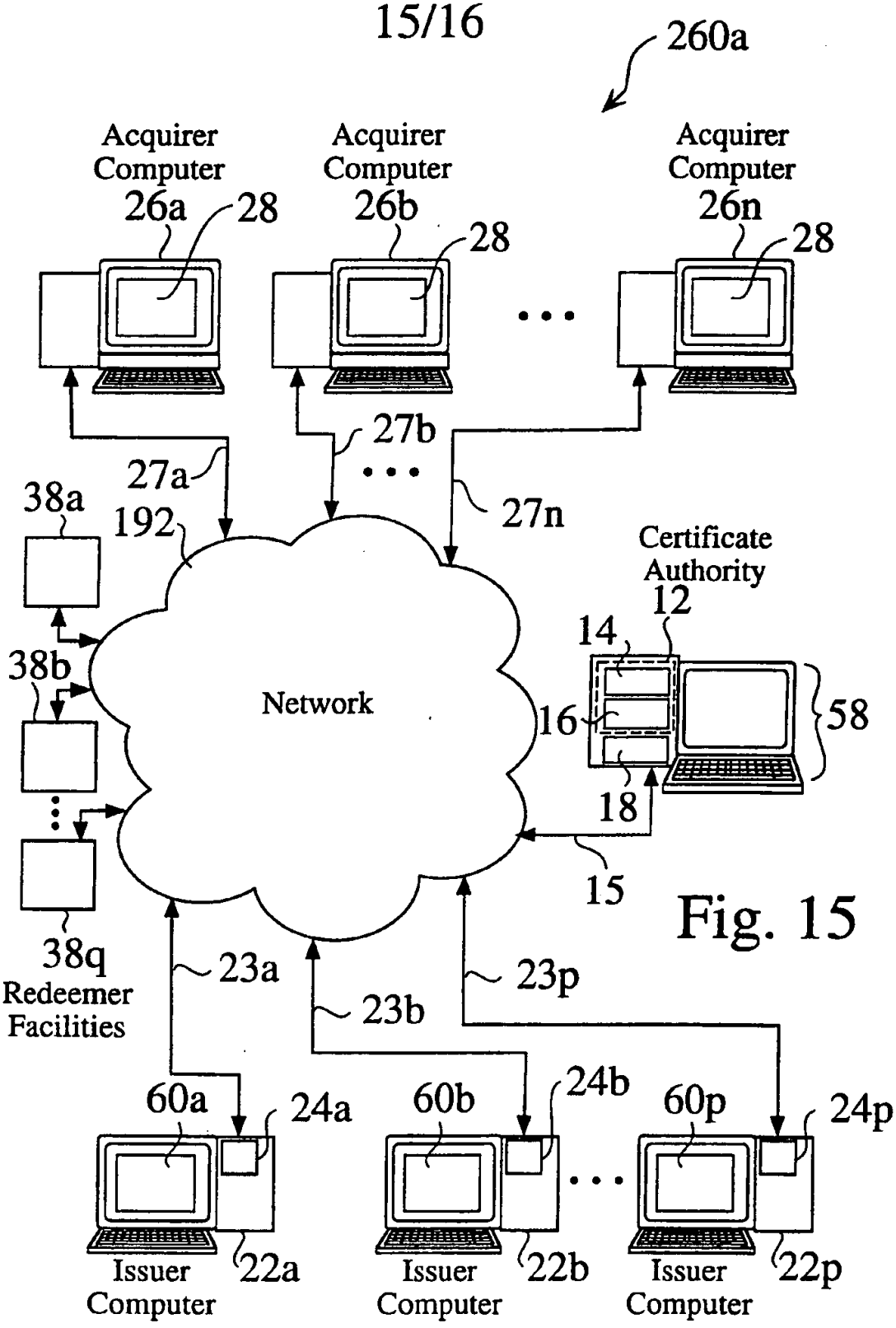

260a
Acquirer Computer
26a
28
Acquirer Computer
26b
28
Acquirer Computer
26n
28
27a
27b
27n
38a
192
38b
38q
Redeemer Facilities
Network
Certificate Authority
12
14
16
18
58
15
23a
23b
23p
60a
24a
22a
Issuer Computer
60b
24b
22b
Issuer Computer
60p
24p
22p
Issuer Computer

Fig. 15

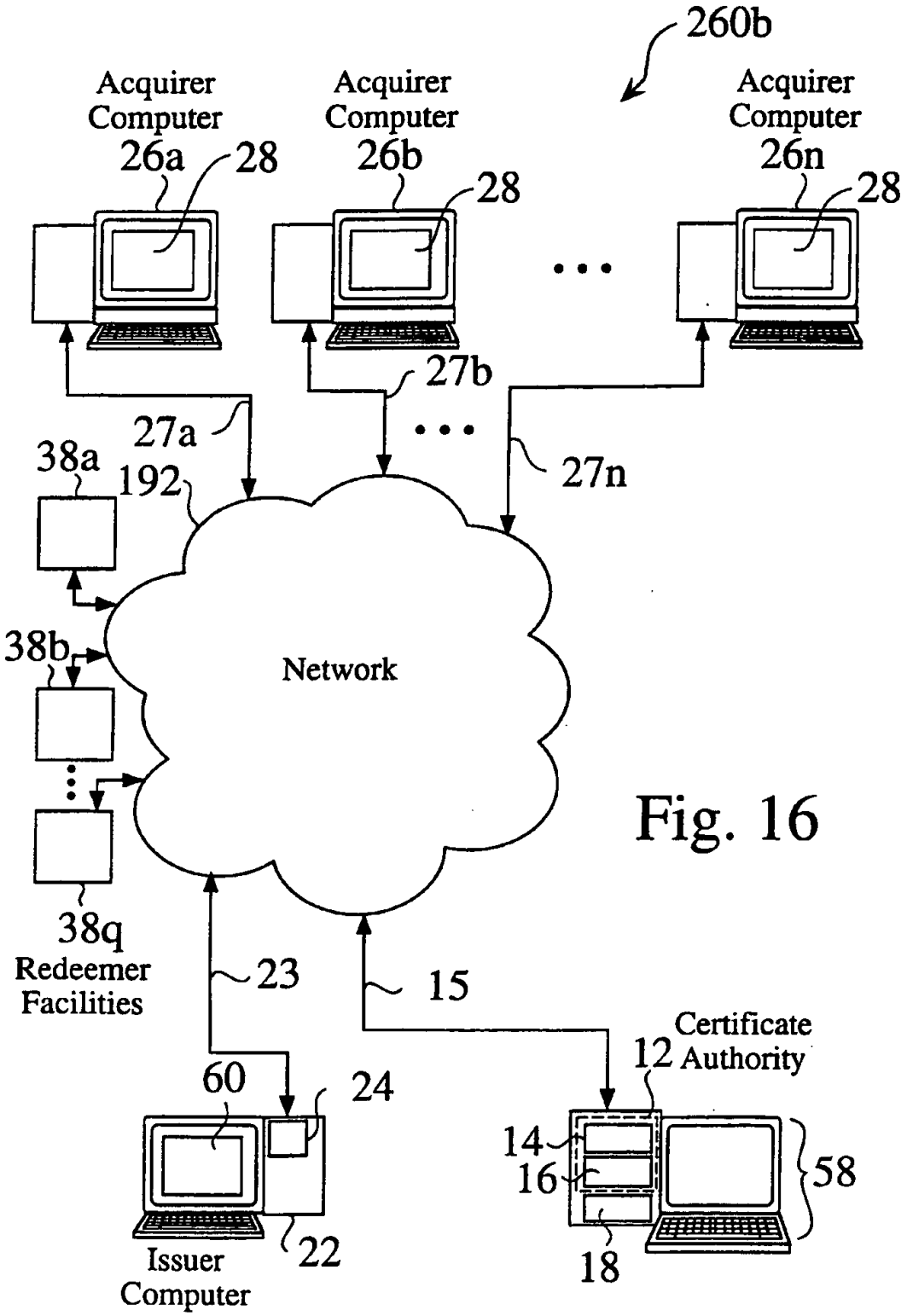

260b
Acquirer Computer
26a
28
Acquirer Computer
26b
28
Acquirer Computer
26n
28
27a
27b
27n
38a
192
38b
Network
38q
Redeemer Facilities
23
15
Certificate Authority
12
60
24
14
16
58
18
22
Issuer Computer

Fig. 16

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 99/30678

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 05555 A (INTERACTIVE COUPON MARKETING GROUP, INC.) 13 February 1997 (1997-02-13)	1,3,4, 6-10,15, 16,18, 19, 21-25,30
A	page 8, line 2 -page 13, line 16	2,5, 11-14, 17,20, 26-29
A	WO 97 23838 A (CATALINA MARKETING INTERNATIONAL, INC.) 3 July 1997 (1997-07-03) the whole document	1-30

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 May 2000	17/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Abram, R

Form PCT/ISA/210 (second sheet) (July 1992)

International Application No
PCT/US 99/30678

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 92 15968 A (THE GIFT CERTIFICATE CENTER, INC.) 17 September 1992 (1992-09-17) the whole document	1-30

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/US 99/30678

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9705555 A	13-02-1997	US 5761648 A	02-06-1998
		AU 710469 B	23-09-1999
		AU 6762796 A	26-02-1997
		BR 9610061 A	27-07-1999
		CA 2227876 A	13-02-1997
		CN 1199479 A	18-11-1998
		EP 0845126 A	03-06-1998
		NZ 315832 A	28-10-1999
WO 9723838 A	03-07-1997	US 5970469 A	19-10-1999
		AU 1344597 A	17-07-1997
		EP 0870264 A	14-10-1998
		JP 11506859 T	15-06-1999
WO 9215968 A	17-09-1992	US 5243174 A	07-09-1993
		AU 649934 B	02-06-1994
		AU 1577492 A	06-10-1992
		CA 2100459 A	06-09-1992
		EP 0574529 A	22-12-1993
		JP 6505582 T	23-06-1994
		MX 9200913 A	01-11-1993
		US 5500514 A	19-03-1996
		US 5652421 A	29-07-1997